

# 1. Definiton of ring

## 1.3

Let  $R$  be a ring, and let  $S$  be any set. Explain how to endow the set  $R^S$  of set-functions  $S \rightarrow R$  of two operations  $+$ , so as to make  $R^S$  into a ring, such that  $R^S$  is just a copy of  $R$  if  $S$  is a sigleton.

**Proof.** The construction is straight forward, for any  $f, g \in R^S$ , let:

$$f + g : S \rightarrow R, s \mapsto f(s) + g(s)$$

$$fg : S \rightarrow R, s \mapsto f(s)g(s)$$

□

## 1.12

Just as complex numbers may be viewed as combinations  $a + bi$ , where  $a, b \in \mathbb{R}$ , and  $i$  satisfies the relation  $i^2 = -1$  (and commutes with  $\mathbb{R}$ ), we may construct a ring  $\mathbb{H}$  by considering linear combinations  $a + bi + cj + dk$  where  $a, b, c, d \in \mathbb{R}$ , and  $i, j, k$  commute with  $\mathbb{R}$  and satisfy the following relations:

$$i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j.$$

Addition in  $\mathbb{H}$  is defined componentwise, while multiplication is defined by imposing distributivity and applying the relations. For example,

$$(1+i+j)(2+k) = 12 + i2 + j2 + 1k + ik + jk = 2 + 2i + 2j + kj + i = 2 + 3i + j + k$$

- (i) Verify that this prescription does indeed define a ring.
- (ii) Compute  $(a + bi + cj + dk)(a - bi - cj - dk)$ , where  $a, b, c, d \in \mathbb{R}$ .
- (iii) Prove that  $\mathbb{H}$  is a division ring  
Elements of  $\mathbb{H}$  are called quaternions. Note that  $\mathbb{Q}_8 := \{\pm 1, \pm i, \pm j, \pm k\}$  forms a subgroup of the group of units of  $\mathbb{H}$ ; it is a noncommutative group of order 8, called the quaternionic group.
- (iv) List all subgroups of  $\mathbb{Q}_8$ , and prove that they are all normal.
- (v) Prove that  $\mathbb{Q}_8, D_8$  are not isomorphic.

**Proof.** The proof is as follows:

- (i) It's obviously the set  $\mathbb{H}$  forms an abelian group where  $0 \in \mathbb{R}$  is the identity and each element  $a + bi + cj + dk$  has addition inverse  $-a - bi - cj - dk$ . For multiplication, the operation is close and has identity 1, and distribution law is natavly true because multiplication is defined in this way.

(ii)

$$\begin{aligned}
 & (a + bi + cj + dk)(a - bi - cj - dk) \\
 &= a^2 - (bi + cj + dk)^2 \\
 &= a^2 - (-b^2 - c^2 - d^2 + bcij + bdik + cdjk + bcji + bdkj + cdkj) \\
 &= a^2 + b^2 + c^2 + d^2
 \end{aligned}$$

- (iii) To prove that  $\mathbb{H}$  is a division ring, it suffices to show that each element is an unit. According to (i), we have

$$(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$$

and:

$$(a - bi - cj - dk)(a + bi + cj + dk) = a^2 + (-b)^2 + (-c)^2 + (-d)^2$$

Thus, the multiplication inverse of  $a + bi + cj + dk$  is  $(a - bi - cj - dk)/(a^2 + b^2 + c^2 + d^2)$

- (iv) Since the order of  $\mathbb{Q}_8$  is 8, the only possible size of the subgroup of  $\mathbb{Q}_8$  could only be 2 and 4. For the first case, it's impossible since no element of  $\mathbb{Q}_8$  has order of 2. For the second case, recall that there are only two possible structure of group with order 4:

The first one is isomorphic to  $\mathbb{Z}_2 \times \mathbb{Z}_2$ , with means there are four elements of order 2, which is impossible as explained before.

The second one is isomorphic to  $\mathbb{Z}_4$ , generated by an element of order 4. Thus, subgroups of 4 are exactly  $\{i, -1, -i, 1\}$  or  $\{j, -1, -j, 1\}$ ,  $\{k, -1, -k, 1\}$ . For any element  $g$  of  $\mathbb{Q}_8$ , we have  $gig^{-1}$  is still an element of this subgroup. Thus this subgroup is normal.

(v) TODO

□

## 1.13

Verify that the multiplication defined in  $R[x]$  is associative.

**Proof.** We have to prove for any  $f(x), g(x), h(x) \in R[x]$ ,  $(f(x)g(x))h(x) = f(x)(g(x)h(x))$ . Suppose that:

$$f(x) = \sum_{i=0}^n a_i x^i, g(x) = \sum_{i=0}^m b_i x^i, h(x) = \sum_{i=0}^l c_i x^i$$

Then for  $(f(x)g(x))h(x)$  the coefficient of  $x^p$  is:

$$\sum_{i+j=p} (fg)_i h_j = \sum_{i+j=p} (fg)_i c_j = \sum_{i+j=p} \left( \sum_{k+l=i} a_k b_l \right) c_j \stackrel{!}{=} \sum_{k+l+j=p} a_k b_l c_j$$

Similarly, for  $f(x)(g(x)h(x))$ , the coefficient of  $x^p$  is:

$$\sum_{i+j=p} f_i (gh)_j = \sum_{i+j=p} f_i \left( \sum_{k+l=j} b_k c_l \right) \stackrel{!}{=} \sum_{i+k+l=p} a_i b_k c_l$$

Note that the equation labeled with ! is induced by the associativity and distributive law of  $R$  itself.  $\square$

### 1.14

Let  $R$  be a ring, and let  $f(x), g(x) \in R[x]$  be nonzero polynomials. Prove that

$$\deg(f(x) + g(x)) \leq \max(\deg(f(x)), \deg(g(x))).$$

Assuming that  $R$  is an integral domain, prove that

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)).$$

**Proof.** Let  $n = \deg(f(x) + g(x))$ , then  $\exists f_i \neq 0, i \geq n$  or  $\exists g_i \neq 0, i \geq n$ . Thus  $\max(\deg(f(x)), \deg(g(x))) \geq \deg(f(x) + g(x))$

For the second part, let  $n = \deg f(x), m = \deg g(x)$ , then  $(fg)_{n+m} = f_n g_m \neq 0$ . And for any  $i > n + m$ , we must have  $(fg)_i = 0$  as  $f_i = 0, i > n$  and  $g_i = 0, i > m$ .  $\square$

### 1.15

Prove that  $R[x]$  is an integral domain if and only if  $R$  is an integral domain

**Proof.** If  $R[x]$  is an integral domain, then  $R$  is an integral domain as  $R$  can be viewed as element of  $R[x]$ . If  $R$  is integral domain, then

$$\deg(fg) = \deg f + \deg g \geq \max(\deg f, \deg g) \geq 0$$

when  $\deg f, \deg g \geq 0$ . Thus  $R[x]$  is an integral domain.  $\square$

## 1.16

Let  $R$  be a ring, and consider the ring of power series  $R[[x]]$

- (i) Prove that a power series  $a_0 + a_1x + a_2x^2 + \dots$  is a unit in  $R[[x]]$  if and only if  $a_0$  is a unit in  $R$ . What is the inverse of  $1x$  in  $R[[x]]$ ?
- (ii) Prove that  $R[[x]]$  is an integral domain if and only if  $R$  is.

**Proof.** The proof is as follows:

- (i) If  $a_0 + a_1x + a_2x^2 + \dots$  has inverse, let the inverse be  $b_0 + b_1x + b_2x^2 + \dots$ , then we have

$$\begin{aligned} 1 &= (a_0 + a_1x + a_2x^2 + \dots)(b_0 + b_1x + b_2x^2 + \dots) \\ &= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots \end{aligned}$$

We must have  $a_0b_0 = 1$ , similarly we have  $b_0a_0 = 1$ . Thus indicates  $a_0$  is an unit.

On the other hand, if  $a_0$  has inverse, we formally write the inverse of  $f$  as:  $f^{-1} = b_0 + b_1x + b_2x^2 + \dots$ . Thus  $ff^{-1} = 1$  implies the followings equations:

$$\begin{aligned} a_0b_0 &= 1 \\ a_0b_1 + a_1b_0 &= 0 \\ a_0b_2 + a_1b_1 + a_2b_0 &= 0 \\ a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 &= 0 \\ &\dots \end{aligned}$$

$g$  is constructed by solve these equations:

$$\begin{aligned} b_0 &= a_0^{-1} \\ b_1 &= -a_0^{-1}a_1b_0 \\ b_2 &= -a_0^{-1}(a_1b_1 + a_2b_0) \\ &\dots \\ b_k &= -a_0^{-1}\left(\sum_{i=1}^k a_i b_{k-i}\right) \end{aligned}$$

This indicates  $f$  is an unit.

- (ii) If  $f, g \in R[[x]]$  and  $f, g \neq 0$ . Then write them in the following form:

$$f = x^p(a_p + a_{p+1}x + \dots), g = x^q(b_q + b_{q+1}x + \dots)$$

Then  $fg = x^{p+q}(a_pb_q + \dots) \neq 0$ . In addition,  $R$  is Commutative indicates  $R[[x]]$  is also commutative, thus  $R[[x]]$  is an integral domain.

□

## 2. Category Ring

### 2.3

Let  $S$  be a set, and consider the power set ring  $\mathcal{P}(S)$  (Exercise 1.2), and the ring  $(\mathbb{Z}/2\mathbb{Z})^S$  you constructed in Exercise 1.3. Prove that these two rings are isomorphic. (Cf. Exercise I.2.11.)

**Proof.** First note that  $\mathcal{P}(S)$  and  $(\mathbb{Z}/2\mathbb{Z})^S$  are isomorphic in **Set**. For each  $f \in (\mathbb{Z}/2\mathbb{Z})^S$ , maps  $f$  to  $\varphi(f)$  by the following subset of  $S$ :

$$\varphi(f) = \{s \in S \mid f(s) = [1]_2\}$$

Then it's easy to show that  $\varphi$  is both bijective and a ring homomorphism, therefore a ring isomorphism.  $\square$

### 2.6

Let  $\alpha : R \rightarrow S$  be a fixed ring homomorphism, and let  $s \in S$  be an element commuting with  $\alpha(r)$  for all  $r \in R$ . Then there is a unique ring homomorphism  $\bar{\alpha} : R[x] \rightarrow S$  extending  $\alpha$ , and sending  $x$  to  $s$

**Proof.** Define  $\bar{\alpha}$  as follows:

$$\bar{\alpha}\left(\sum_{i \geq 0} a_i x^i\right) = \sum_{i \geq 0} \alpha(a_i) s^i$$

To prove this is a ring homomorphism, we need to show that  $\bar{\alpha}$  maintains both addition and multiplication (and send identity to identity, which is obvious). Addition is easy to verify, for multiplication, it is worthy noted  $s$  commutes with  $\alpha(r)$ ,  $r \in R$  makes it maintains multiplication:

$$\begin{aligned} \bar{\alpha}\left(\left(\sum_{i \geq 0} a_i x^i\right)\left(\sum_{i \geq 0} b_i x^i\right)\right) &= \bar{\alpha}\left(\sum_{i \geq 0} \left(\sum_{k+l=i} a_k b_l\right) x^i\right) = \sum_{i \geq 0} \alpha\left(\sum_{k+l=i} a_k b_l\right) s^i \\ \bar{\alpha}\left(\sum_{i \geq 0} a_i x^i\right) \bar{\alpha}\left(\sum_{i \geq 0} b_i x^i\right) &= \left(\sum_{i \geq 0} \alpha(a_i) s^i\right) \left(\sum_{i \geq 0} \alpha(b_i) s^i\right) \\ &= \sum_{i \geq 0} \left(\sum_{k+l=i} \alpha(a_k) s^k \alpha(b_l) s^l\right) \\ &\stackrel{!}{=} \sum_{i \geq 0} \left(\sum_{k+l=i} \alpha(a_k) \alpha(b_l) s^i\right) \\ &= \sum_{i \geq 0} \left(\alpha\left(\sum_{k+l=i} a_k b_l\right) s^i\right) \\ &= \bar{\alpha}\left(\left(\sum_{i \geq 0} a_i x^i\right)\left(\sum_{i \geq 0} b_i x^i\right)\right) \end{aligned}$$

Note that ! is true because  $s$  commutes with all  $\alpha(a_k)$  and  $\alpha(b_l)$ . The uniqueness of  $\bar{\alpha}$  comes from the fact that  $\bar{\alpha}$  is homomorphism, and  $\bar{\alpha}(r) = \alpha(r)$ ,  $\bar{\alpha}(x) = s$ .  $\square$

**NOTE** Example 2.2 asks for particular situation, where a ring homomorphism  $\varphi : \mathbb{Z}[x] \rightarrow S$  extends the unique homomorphism  $f : \mathbb{Z} \rightarrow S, n \mapsto n1_S$  and sends  $x$  to any element of  $S$  doesn't necessarily consider the commutativity of  $S$ . The answer is clean here, any element  $s \in S$  must commutes with the image of  $f$  since  $s(n1_S) = ns = (n1_S)s$

## 2.9

The center of a ring  $R$  consists of the elements  $a$  such that  $ar = ra$  for all  $r \in R$ . Prove that the center is a subring of  $R$ . Prove that the center of a division ring is a field.

**Proof.** Denote the center of  $R$  as  $Z(R)$ , then for any  $s, t \in Z(R), r \in R$ , we have  $r(s-t) = rs - rt = sr - tr = (s-t)r$ , which indicates that  $s-t \in Z(R)$ . Thus,  $Z(R)$  is an addition subgroup of  $R$ .

Moreover,  $\forall s, t \in Z(R), r \in R$ , we have  $(st)r = s(tr) = s(rt) = (sr)t = (rs)t = r(st)$ . Thus  $rs \in Z(R)$ , indicating  $Z(R)$  is closed under multiplication. The associativity and distributive law naturally holds in  $Z(R)$ . And  $1_R \in Z(R)$  obviousl. In conclusion,  $Z(R)$  is a subring of  $R$ .

If  $R$  is a division ring, for any  $s \in Z(R)$ , we must prove that  $s^{-1} \in Z(R)$ . Actually, for any  $s \in Z(R), r \in R, sr = rs \Rightarrow rs^{-1} = s^{-1}r$ . Thus  $s^{-1} \in Z(R)$ . And  $Z(R)$  is obviously commutative, and therefore a field.  $\square$

## 2.10

The *centralizer* of an element  $a$  of a ring  $R$  consists of the elements  $r \in R$  such that  $ar = ra$ . Prove that the centralizer of  $a$  is a subring of  $R$ , for every  $a \in R$ . Prove that the center of  $R$  is the intersection of all its centralizers. Prove that every centralizer in a division ring is a division ring.

**Proof.** To prove the centralizer of  $a \in R$  is a subring of  $R$  basically follows the same way as exercise 2.9 does.

For the second part, if  $s \in Z(R)$ , then  $s$  commutes with any element  $r \in R$ , thus  $s \in \text{Cen}_R(r), r \in R$ . and  $s \in \bigcap_{r \in R} \text{Cen}_R(r)$ , indicating  $Z(R) \subseteq \bigcap_{r \in R} \text{Cen}_R(r)$ . On the other hand, any element of  $\bigcap_{r \in R} \text{Cen}_R(r)$  must commute with any element of  $R$ , thus belongs to  $Z(R)$ . In conclusion,

$$Z(R) = \bigcap_{r \in R} \text{Cen}_R(r).$$

For the third part, it suffices to show that if  $r$  commutes with  $a$  then so does  $r^{-1}$ . It is done in exercise 2.9 already.  $\square$

## 2.11

Let  $R$  be a division ring consisting of  $p^2$  elements, where  $p$  is a prime. Prove that  $R$  is commutative.

**Proof.** Assume that  $R$  is not commutative, consider the center of  $R$ , denoted as  $Z(R)$ . Then  $Z(R) \neq R$ . Note that  $Z(R)$  is an addition subgroup of  $R$ . Then it must have  $|Z(R)| = p$  since  $|Z(R)|$  divides  $|R|$ , which is  $p^2$ .

Consider one element  $r \in R, r \notin Z(R)$ , and its centralizer, denoted as  $\text{Cen}_R(r)$ , then since  $r \notin Z(R)$ , it means  $\text{Cen}_R(r) \neq R$ . And exercise 2.10 indicates  $\text{Cen}_R(r)$  is a subring of  $R$ , thus  $|\text{Cen}_R(r)| = p$ .

Exercise 2.10 also shows that  $Z(R) \subseteq \text{Cen}_R(r)$ , their cardinality equals to each other means  $Z(R) = \text{Cen}_R(r)$ . However, it's obvious that  $r \in \text{Cen}_R(r)$  but  $r \notin Z(R)$ , a contradiction.

In conclusion, we must have  $Z(R) = R$  and  $R$  is therefore commutative, further more, it's a field.  $\square$

**NOTE** In fact, any finite division ring is commutative, thus a field. But the proof used here seems hard to extend to more complex condition, i.e. the case of arbitrary integer. Actually, it's even hard to extend this method to  $p^n, n \geq 3$  case:  $|Z(R)|$  might be  $p^3$  and  $\text{Cen}_R(r)$  might be  $p^2$  and no contradictions so far.

## 2.12

Consider the inclusion map  $\iota : \mathbb{Z} \rightarrow \mathbb{Q}$ . Describe the cokernel of  $\iota$  in **Ab**, and its cokernel in **Ring** (as defined by the appropriate universal property in the style of the one given in § II.8.6)

**Proof.** Before we describe the cokernel requested above, we will review what these concepts (and kernel) means in category conception:

**Kernel** Let  $G, H$  be group and  $f : G \rightarrow H$  is a group homomorphism.

Then Consider the following category:  $\mathcal{K}_\varphi$ : The object of  $\mathcal{K}_\varphi$  is one group  $S$  associated one morphism  $j$ , such that the following diagram holds:

$$\begin{array}{ccccc} & & 0 & & \\ & \searrow & \text{---} & \nearrow & \\ S & \xrightarrow{j} & G & \xrightarrow{f} & H \end{array}$$

And the morphism between  $(j_1, S_1)$  and  $(j_2, S_2)$  is the following diagram:

$$\begin{array}{ccccc} & & 0 & & \\ & \searrow & \text{---} & \nearrow & \\ S_2 & \xrightarrow{j_2} & G & \xrightarrow{f} & H \\ & \swarrow \varphi & \uparrow j_1 & & \\ & & S_1 & & \end{array}$$

And  $\ker \varphi$  is defined to be the final object of  $\mathcal{K}_\varphi$ . That is, the following diagram holds:

$$\begin{array}{ccccc} & & 0 & & \\ & \searrow & \text{---} & \nearrow & \\ \ker f & \xrightarrow{\iota} & G & \xrightarrow{f} & H \\ & \swarrow \exists! \varphi & \uparrow j & & \\ & & S & & \end{array}$$

And  $\ker f$  exists as  $\ker f = \{g \in G \mid f(g) = 0\}$ . It's easy to verify such set is a subgroup of  $G$  and this subgroup associated with the injection homomorphism satisfies the universal property of  $\ker$ .

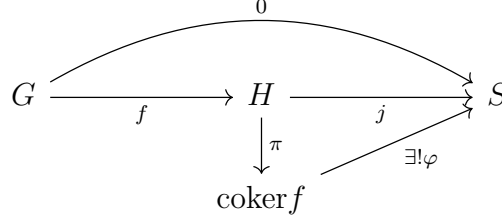
**Cokernel** Conceptually, cokernel just reverse all arrows in the above diagram. Let  $G, H$  be groups and  $f : G \rightarrow H$  is a group homomorphism, consider the category  $\mathcal{C}_f$  of which objects and morphisms are following diagrams:

$$\begin{array}{ccccc} & & 0 & & \\ & \searrow & \text{---} & \nearrow & \\ G & \xrightarrow{f} & H & \xrightarrow{j_2} & S_2 \\ & & \downarrow j_1 & \nearrow \varphi & \\ & & S_1 & & \end{array}$$

And  $\text{coker } f$  is an initial object in this category, that is, the following diagram



holds:



As we have proved before, in **Grp**,  $\text{coker } f$  is  $H/N$ , where  $N$  is the smallest normal subgroup that contains  $\text{Im } f$ . In particular,  $\text{coker } f = H/\text{Im } f$  in **Ab**.

If we replace groups with rings and group homomorphisms with ring homomorphisms, we can naturally get the definition of kernel and cokernel in **Ring**.

Now back to the problem itself,  $\text{coker } \iota$  in **Ab**, as stated, is  $\mathbb{Q}/\mathbb{Z}$ . The associated  $\pi$  is  $\pi(q) = q + \mathbb{Z}$ . And  $\text{coker } \iota$  in **Ring** is  $(0, \{0\})$ . Actually if  $(j, S)$  where  $S$  is a ring and  $j$  is a ring homomorphism from  $\mathbb{Q}$  to  $S$ , if it satisfies  $j \circ \iota = 0$ . Then we have:

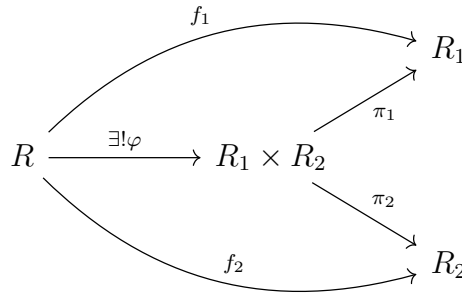
$$j\left(\frac{p}{q}\right) = j(pq^{-1}) = j(p)j(q)^{-1} = j(\iota(p))j(\iota(q)) = 0(p)0(q)^{-1} = 0$$

Thus  $j$  maps each element to be 0 in  $S$ , thus  $S$  could only be  $\{0\}$  since  $1_S = f(1_{\mathbb{Q}}) = 0$ . This indicates there is only one object in this category, and  $\text{coker } \iota$  is this object.  $\square$

## 2.13

Verify that the ‘componentwise’ product  $R_1 \times R_2$  of two rings satisfies the universal property for products in a category, given in § I.5.4

**Proof.**  $(R_1 \times R_2, \pi_1, \pi_2)$  is the product of  $R_1$  and  $R_2$ , where  $\pi_1(r_1, r_2) = r_1$  and  $\pi_2(r_1, r_2) = r_2$ . It’s easy to show that  $\pi_1, \pi_2$  are ring homomorphisms, we must show that the following diagrams holds:



For  $(R, f_1, f_2)$ , defines  $\varphi : R \rightarrow R_1 \times R_2, r \mapsto (f_1(r), f_2(r))$ . Then the diagram is commutative. To prove the uniqueness, consider another ring homomorphism  $\varphi' : R \rightarrow R_1 \times R_2$  makes this diagram commutes, then  $\varphi'(r) = (r_1, r_2)$ . Further we have  $f_1(r) = \pi_1(\varphi(r)) = \pi_1(r_1, r_2) = r_1, f_2(r) = \pi_2(\varphi(r)) = \pi_2(r_1, r_2) = r_2$ . Thus  $\varphi(r) = (f_1(r), f_2(r))$ , the uniqueness is proved.

In conclusion,  $(R_1 \times R_2, \pi_1, \pi_2)$  is the product of  $R_1$  and  $R_2$ .  $\square$

## 2.16

Prove that there is (up to isomorphism) only one structure of ring with identity on the abelian group  $(\mathbb{Z}, +)$ .

## 3.Ideals and quotient rings

### 3.2

Let  $\varphi : R \rightarrow S$  be a ring homomorphism, and let  $J$  be an ideal of  $S$ . Prove that  $I = \varphi^{-1}(J)$  is an ideal of  $R$ . Thus, the inverse image of an image is also an ideal, is the image of an ideal also an ideal? Prove it or given a counterexample.

**Proof.** For any  $s \in \varphi^{-1}(J), r \in R$ , we have  $\varphi(rs) = \varphi(r)\varphi(s) \in J, \varphi(sr) = \varphi(s)\varphi(r) \in J$  since  $\varphi(s) \in J, \varphi(r) \in R$ , which indicates that  $rs \in \varphi^{-1}(J), sr \in \varphi^{-1}(J)$ . Thus  $\varphi^{-1}(J)$  is an ideal.

Then second proposition is false in general, the ring homomorphism image of an ideal is not necessarily an ideal. Consider injection:  $\iota : \mathbb{Z} \rightarrow \mathbb{Z}[x]$ . However, the image of an ideal, say  $2\mathbb{Z}$  is still  $2\mathbb{Z} \subseteq \mathbb{Z}[x]$  and is not an ideal of  $\mathbb{Z}$ .

However, if  $\varphi$  is surjective, then  $\varphi(I)$  is also an ideal of the target ring.  $\square$

### 3.3

Let  $\varphi : R \rightarrow S$  be a ring homomorphism, and let  $J$  be an ideal of  $R$ .

1. Show that  $\varphi(J)$  need not be an ideal of  $S$ .
2. Assume that  $\varphi$  is surjective; then prove that  $\varphi(J)$  is an ideal of  $S$ .
3. Assume that  $\varphi$  is surjective, and let  $I = \ker \varphi$ ; thus we may identify  $S$  with  $R/I$ . Let  $\bar{J} = \varphi(J)$ , an ideal of  $R/I$  by the previous point. Prove

that

$$\frac{R/I}{\bar{J}} \cong \frac{R}{I+J}$$

**Proof.** The first proposition are proved in exercise 3.2, and the second one is easy to be proved following the definition.

For the third proposition, note that actually we have  $\bar{J} \cong (I+J)/J$ , then according to proposition 3.14, we have:

$$\frac{R/I}{\bar{J}} \cong \frac{R/J}{(I+J)/J} \cong R/(I+J)$$

The proof is done.  $\square$

### 3.4

Let  $R$  be a ring such that every subgroup of  $(R, +)$  is in fact an ideal of  $R$ . Prove that  $R \cong \mathbb{Z}/n\mathbb{Z}$ , where  $n$  is the characteristic of  $R$

**Proof.** Consider the subset:

$$S = \{n1_R \mid n \in \mathbb{Z}\}$$

It is a subgroup of  $(R, +)$  because:

$$(\forall a1_R, b1_R \in S, a, b \in \mathbb{Z}) : \quad a1_R - b1_R = (a - b)1_R \in S$$

According to the assumption, we have  $S$  to be an ideal, in particular, we have:

$$(\forall r \in R) : \quad r = r1_R \in S$$

this indicates that  $\forall r \in R, r = m1_R$  for some  $m \in \mathbb{Z}$ . And therefore  $R = S$ . This indicates  $R \cong \mathbb{Z}$  or  $R \cong \mathbb{Z}/n\mathbb{Z}$  for  $n$  to be the characteristic of  $R$ .  $\square$

### 3.8

Prove that a ring  $R$  is a division ring if and only if its only left-ideals and right-ideals are  $\{0\}$  and  $R$ . In particular, a commutative ring  $R$  is a field if and only if the only ideals of  $R$  are  $\{0\}$  and  $R$ .

**Proof.** Let  $R$  be a ring, and  $I$  be an ideal of  $R$ . Then if  $I$  contains element other than  $0_R$ , we will have  $I = R$  since  $1_R \in I$ . Thus the ideal of  $R$  can only be  $R$  and  $\{0\}$  if  $R$  is a division ring.

On the other hand, if  $R$  has only  $\{0\}$  and  $R$  as ideals, then any element of  $R$  must be an unit, otherwise  $aR$  where  $a$  is a non-unit, could be a right-ideal, a contradiction.

The second part of this problem is nothing more than a special case of field.  $\square$

### 3.9

Counterpoint to Exercise 3.8: it is not true that a ring  $R$  is a division ring if and only if its only two-sided ideals are  $\{0\}$  and  $R$ . A nonzero ring with this property is said to be simple; by Exercise 3.8, fields are the only simple commutative rings.

**Proof.** If  $R$  is a division ring, then the ideals of  $R$  could only be  $R$  or  $\{0\}$ . However, the ideals of  $R$  are only  $\{0\}$  and  $R$  doesn't mean both left-ideals and right-ideals of  $R$  are only  $\{0\}$  and  $R$ .  $\square$

### 3.11

Let  $R$  be a ring containing  $\mathbb{C}$  as a subring. Prove that there are no ring homomorphisms  $R \rightarrow \mathbb{R}$

**Proof.** If there exists some ring homomorphism  $R \rightarrow \mathbb{R}$ , then it induce a ring homomorphism from  $\mathbb{C}$  to  $\mathbb{R}$ . However, this can not be true because:

$$-1 = f(-1) = f(\mathbf{i} * \mathbf{i}) = f(\mathbf{i})^2$$

There is no such  $f(\mathbf{i}) \in \mathbb{R}$  satisfies  $f(\mathbf{i})^2 = -1$   $\square$

### 3.12

Let  $R$  be a commutative ring. Prove that the set of nilpotent elements of  $R$  is an ideal of  $R$ . (Cf. Exercise 1.6. This ideal is called the *nilradical* of  $R$ .) Find a non-commutative ring in which the set of nilpotent elements is not an ideal.

**Proof.** Let  $N$  denotes the set of all nilpotent elements of  $R$ , first to prove that  $N$  is a subgroup of  $(R, +)$ . For any  $a, b \in N$ , there exists some  $m, n \in \mathbb{N}^+$  that  $a^m = 0, b^n = 0$ , then we shall have  $(a - b)^{m+n+1} = 0$  (using binomial theorem). This indicates  $a - b \in N$ , and thus  $N$  is a subgroup of  $(R, +)$ .

The second part is to prove that for any  $r \in R, a \in N, ra \in N$ . Note that  $(ra)^m = r^m a^m = r^m 0 = 0$ . Thus  $ra \in N$ . In conclusion, we have  $N$  is an ideal of  $R$ .

One counterexample for non-commutative case would be matrix ring  $M_n(\mathbb{R})$ . Note that  $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$  is a nilpotent element but  $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$  is not, which fails to make  $N(M_n(\mathbb{R}))$  to be an ideal.

**NOTE** There might be some properties of this ideal, one most notable is that the quotient ring  $R/N$  has no non-naive nilpotent element:

$$(a + N)^m = 0_{R/N} \Rightarrow a^m + N = 0_{R/N} \Rightarrow a^m \in N \Rightarrow a \in N$$

□

### 3.13

Let  $R$  be a commutative ring, and let  $N$  be its nilradical (cf. Exercise 3.12). Prove that  $R/N$  contains no nonzero nilpotent elements. (Such a ring is said to be reduced.)

**Proof.** The proof is done in the "NOTE" section of exercise 3.12 □

### 3.14

Prove that the characteristic of an integral domain is either 0 or a prime integer. Do you know any ring of characteristic 1?

**Proof.** If the characteristic of  $R$  is non-prime, say  $\text{char} R = mn, m > 1, n > 1$ . Then the definition of characteristic shows that  $mn1_R = 0$ , which is  $(m1_R)(n1_R) = 0$ . Note that  $m > 1, n > 1$  indicates  $m < \text{char} R, n < \text{char} R$ , thus  $m1_R \neq 0, n1_R \neq 0$ . The equation  $(m1_R)(n1_R) = 0$  implies the multiplication of two non-zero elements is zero, which contradicts the definition of integral domain.

Ring of characteristic 1 could only be zero ring. □

### 3.15

A ring  $R$  is *boolean* if  $a^2 = a$  for all  $a \in R$ . Prove that  $\mathcal{P}(S)$  is boolean, for every set  $S$  (cf. Exercise 1.2). Prove that every boolean ring is commutative, and has characteristic 2. Prove that if an integral domain  $R$  is boolean, then  $R \cong \mathbb{Z}/2\mathbb{Z}$

**Proof.**  $\mathcal{P}(S)$  is boolean as for any element  $S \in \mathcal{P}(S)$  we have  $S^2 = S \cap S = S$ . First we prove that if  $R$  is *boolean*, then for each element  $r \in R$ , we have  $2r = 0$ , thus the characteristic of  $R$  is 2. Consider the following two equations:

$$(1 + r) = (1 + r)^2 = 1 + 2r + r^2 = 1 + 2r + r$$

This indicates  $\forall r \in R, 2r = 0$ . Further,  $\forall a, b \in R$ , we have:

$$(a + b) = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$$

This means  $ab + ba = 0$ , note that  $2ab = 0$ , these two equations imply  $ab = ba, \forall a, b \in R$ . Thus  $R$  is commutative. The characteristic part is proved already.

If  $R$  is itself an integral domain, then for any element  $r \in R$ , we have:

$$r^2 = r \Rightarrow r(r - 1_R) = 0 \Rightarrow r = 1_R$$

This implies there are only two elements of  $R$  if it is boolean and domain, thus is isomorphic to  $\mathbb{Z}/2\mathbb{Z}$ .  $\square$

### 3.17

Let  $I, J$  be ideals of a ring  $R$ . State and prove a precise result relating the ideals  $(I + J)/I$  of  $R/I$  and  $J/(I \cap J)$  of  $R/(I \cap J)$

**Proof.**  $(I + J)/I$  is an ideal of quotient ring  $R/I$ . It's obvious that  $I + J$  is an ideal that contains  $I$ . And there is, actually a one-to-one correspondence between the ideal of  $R/I$  and the ideal of  $R$  that contains  $I$ .

Considering the canonical project:  $\pi : R \rightarrow R/I, r \mapsto r + I$ . The for each ideal of  $R/I$ , say  $S$ ,  $\pi^{-1}(S)$  is an ideal of  $R$  and it contains  $I$ . This map:  $S \mapsto \pi^{-1}(S)$  has one inverse function:  $J \mapsto J/I$ . Thus the bijection exists.  $\square$

## 4. Ideals and quotients: remarks and examples

### 4.2

Prove that the homomorphic image of a Noetherian ring is Noetherian. That is, prove that if  $\varphi : R \rightarrow S$  is a surjective ring homomorphism, and  $R$  is Noetherian, then  $S$  is Noetherian.

**Proof.** Recall that Noetherian ring is a ring where all ideals are finitely generated. Let  $J$  be an ideal of  $S$ , then  $I = \varphi^{-1}(J)$  is an ideal of  $R$ . Then  $R$  is finitely generated, say  $I = (r_1, r_2, \dots, r_n)$ . Then for any element  $p \in J$ , we have  $p = \varphi(q)$ ,  $q \in I$ , thus  $q = \sum_{i=1}^n a_i r_i$  and  $p = \varphi(q) = \sum_{i=1}^n \varphi(a_i) \varphi(r_i)$ . Thus,  $J \subseteq (\varphi(r_1), \varphi(r_2), \dots, \varphi(r_n))$  And is finitely generated.  $\square$

## 4.5

Let  $I, J$  be ideals in a ring  $R$ , such that  $I + J = (1)$ . Prove that  $IJ = I \cap J$

**Proof.** Recall that  $IJ$  denotes the ideal generated by all production  $ij, i \in I, j \in J$ . And  $IJ \subseteq I \cap J$  in general. We have to show  $I \cap J \subseteq IJ$ . For any element  $r \in I \cap J$ , we have  $r = r1_R = r(i + j) = ri + rj, i \in I, j \in J$ . Note that  $ri = ir \in IJ, rj \in IJ$ , thus  $r = ri + rj \in IJ$ , and we have  $IJ \subseteq I \cap J$  as a result.  $\square$

## 4.6

Let  $I, J$  be ideals in a ring  $R$ . Assume that  $R/(IJ)$  is reduced (that is, it has no nonzero nilpotent elements; cf. Exercise 3.13). Prove that  $IJ = I \cap J$ .

**Proof.** If  $IJ \subsetneq I \cap J$ , then there is some element  $r \in I \cap J, r \notin IJ$ . Then consider  $r + IJ \in R/(IJ)$ . We are gonna to have

$$(r + IJ)^2 = r^2 + IJ = IJ$$

as  $r^2 \in IJ (r \in I, r \in J)$ , which contradicts the assumption that  $R/(IJ)$  is reduced. In conclusion,  $IJ = I \cap J$ .  $\square$

## 4.9

Generalize the result of Exercise 4.8, as follows. Let  $R$  be a ring, and let  $f(x)$  be a left-zero-divisor in  $R[x]$ . Prove that  $\exists b \in R, b \neq 0$ , such that  $f(x)b = 0$ .

**Proof.** We prove by induction on the degree of  $f(x)$ . If  $\deg f(x) = 0$ , then  $f(x)$  is simply an element of  $R$ , written as  $r$ . Say  $f(x)g(x) = 0, g(x) \neq 0$ . Then it's easy to see the first coefficient of  $g(x)$ , say  $t$ , satisfies  $rt = 0$ . Thus the proposition is true of  $\deg f(x) = 0$ .

Assume that for  $\deg f(x) = k$  the proposition is true. Then for  $k + 1$  case,  $\square$

## 4.10

Let  $d$  be an integer that is not the square of an integer, and consider the subset of  $\mathbb{C}$  defined by:

$$\mathbb{Q}(\sqrt{d}) := \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

1. Prove that  $\mathbb{Q}(\sqrt{d})$  is a subring of  $\mathbb{C}$ .
2. Define a function  $N : \mathbb{Q}(\sqrt{d}) \rightarrow \mathbb{Z}$  by  $N(a + b\sqrt{d}) := a^2 - b^2d$ . Prove that  $N(zw) = N(z)N(w)$ , and that  $N(z) \neq 0$  if  $z \in \mathbb{Q}(\sqrt{d})$ ,  $z \neq 0$ .
3. Prove that  $\mathbb{Q}(\sqrt{d})$  is a field, and in fact the smallest subfield of  $\mathbb{C}$  containing both  $\mathbb{Q}$  and  $\sqrt{d}$  (Use  $N$ ).
4. Prove that  $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[t]/(t^2 - d)$ . (Cf. Example 4.8.)

The function  $N$  is a ‘norm’; it is very useful in the study of  $\mathbb{Q}(\sqrt{d})$  and of its subrings. (Cf. also Exercise 2.5.)

**Proof.** The proof is as follows:

1.  $\mathbb{Q}(\sqrt{d})$  is indeed a subring of  $\mathbb{C}$  because it’s a subgroup of  $\mathbb{C}$  and closed under multiplication:

$$(\forall a_1 + b_1\sqrt{d}, a_2 + b_2\sqrt{d} \in \mathbb{Q}(\sqrt{d})) :$$

$$(a_1 + b_1\sqrt{d}) - (a_2 + b_2\sqrt{d}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{d} \in \mathbb{Q}(\sqrt{d})$$

$$(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d} \in \mathbb{Q}(\sqrt{d})$$

Also,  $1_{\mathbb{C}} \in \mathbb{Q}(\sqrt{d})$  by setting  $a = 1, b = 0$ . In conclusion,  $\mathbb{Q}(\sqrt{d})$  is a subring of  $\mathbb{C}$ .

2. For the second part, let  $z = a_1 + b_1\sqrt{d}, w = a_2 + b_2\sqrt{d}$ . Then:

$$\begin{aligned} N(zw) &= (a_1a_2 + b_1b_2d)^2 - d(a_1b_2 + a_2b_1)^2 \\ &= a_1^2a_2^2 + b_1^2b_2^2d^2 - da_1^2b_2^2 - da_2^2b_1^2 \\ &= (a_1^2 - b_1^2d)(a_2^2 - b_2^2d) \\ &= N(z)N(w) \end{aligned}$$

If  $N(z) = 0$ , then  $a^2 - b^2d = 0 \Rightarrow a/b = \sqrt{d}$ , contradicts the fact that  $\sqrt{d}$  is irrational.



3.  $\mathbb{Q}(\sqrt{d})$  is a field since each non-zero element  $a + b\sqrt{d}$  has inverse  $(a - b\sqrt{d})/(a^2 - b^2d)$ . Note that we have proved that in (2),  $N(z) = a^2 - b^2d = 0$  if and only if  $z = 0$ , thus it's ok to write  $a^2 - b^2d$  as denominator.
4. Note that  $\mathbb{Q}[t]/(t^2 - d) \cong \mathbb{Q}^{\oplus 2}$ , there is a one to one correspondence:

$$\mathbb{Q}(\sqrt{d}) \rightarrow \mathbb{Q}^{\oplus 2} : a + b\sqrt{d} \mapsto (a, b)$$

And the multiplication defined over  $\mathbb{Q}^{\oplus 2}$  is  $(a, b)(e, f) = (ae + dbf, af + be)$

□