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 $S \to R$ 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:

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

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

□

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 nativaly true because multiplication is defined in this way.

(ii)

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

(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:

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

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

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

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

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

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

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 $g_i = 0, i > m$. □

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

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

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

1.16

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

(i) Prove that a power series $a_0 + a_1x + a_2x^2 + \ldots$ 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 $a_0 + a_1x + a_2x^2 + \ldots$ has inverse, let the inverse be $b_0 + b_1x + b_2x^2 + \ldots$, then we have

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

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: $f^{-1} = b_0 + b_1x + b_2x^2 + \ldots$. Thus $ff^{-1} = 1$ implies the followsing equations:

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

g is constructed by solve these equations:

$$\begin{aligned} b_0 &= a_0^{-1} \\ b_1 &= -a_0^{-1}a_1b_0 \\ b_2 &= -a_0^{-1}(a_1b_1 + a_2b_0) \\ &\ldots \\ b_k &= -a_0^{-1}(\sum_{i=1}^{k} a_ib_{k-i}) \end{aligned}$$

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:

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

Then $fg = x^{p+q}(a_pb_q + \ldots) \neq 0$. 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 $\mathscr{P}(S)$ (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 $\mathscr{P}(S)$ and $(\mathbb{Z}/2\mathbb{Z})^S$ are isomorphic in **Set**. For each $f \in (\mathbb{Z}/2\mathbb{Z})$, 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 φ is both bijective and a ring homomorphim, therefore a ring isomorphism. □

2.6

Let $\alpha : R \to S$ 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 $\overline{\alpha} : R[x] \to S$ extending α, and sending x to s

Proof. Define $\overline{\alpha}$ as follows:

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

To prove this is a ring homomorphism, we need to show that $\overline{\alpha}$ 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 conmmutes with $\alpha(r), r \in R$ makes it maintains multiplication:

$$\overline{\alpha}((\sum_{i\geq 0} a_i x^i)(\sum_{i\geq 0} b_i x^i)) = \overline{\alpha}(\sum_{i\geq 0}(\sum_{k+l=i} a_k b_l)x^i) = \sum_{i\geq 0} \alpha(\sum_{k+l=i} a_k b_l)s^i$$

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

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

NOTE Example 2.2 asks for particular situation, where a ring homomorphism $\varphi : \mathbb{Z}[x] \to S$ extends the unique homomorphism $f : \mathbb{Z} \to S, n \mapsto n1_S$ 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 natively 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 r commutes with any element $r \in R$, thus $s \in \mathrm{Cen}_R(r), r \in R$. and $s \in \bigcap_{r\in R} \mathrm{Cen}_R(r)$, indicating $Z(R) \subseteq \bigcap_{r\in R} \mathrm{Cen}_R(r)$. On the other hand, any element of $\bigcap_{r\in R} \mathrm{Cen}_R(r)$ must commute with any element of R, thus belongs to $Z(R)$. In conclusion,

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

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 $\mathrm{Cen}_R(r)$, then since $r \notin Z(R)$, it means $\mathrm{Cen}_R(r) \neq R$. And exercise 2.10 indicates $\mathrm{Cen}_R(r)$ is a subring of R, thus $|\mathrm{Cen}_R(r)| = p$.

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

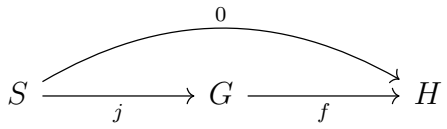
NOTE In fact, any finite division ring is commutative, thus a field. But the proof used here seems hard to extend to more complex condition, i.e. the case of arbitary integer. Actually, it's even hard to extend this method to $p^n, n \geq 3$ case: $|Z(R)|$ might be p^3 and $\mathrm{Cen}_R(r)$ might be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

2.12

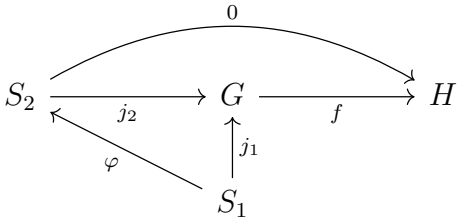
Consider the inclusion map $\iota : \mathbb{Z} \to \mathbb{Q}$. Describe the cokernel of ι in **Ab**, and its cokernel in **Ring** (as defined by the appropriate universal property in the style of the one given in § II.8.6)

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 $f : G \to H$ is a group homomorphism.

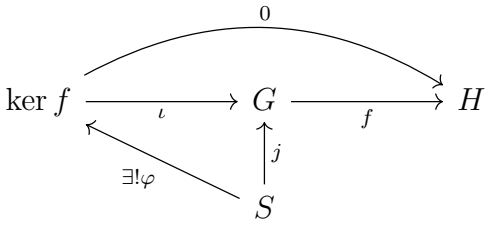
Then Consider the following category: $\mathscr{K}_\varphi$: The object of $\mathscr{K}_\varphi$ is one group S associated one morphism j, such that the following diagram holds:



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

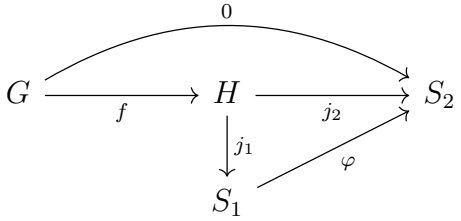


And $\ker\varphi$ is defined to be the final object of $\mathscr{K}_\varphi$. That is, the following diagram holds:



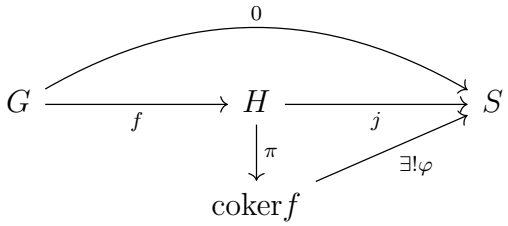
And $\ker f$ exists as $\ker f = \{g \in G \mid f(g) = 0\}$. It's easy to verify such set is a subgroup of G and this subgroup associated with the injection homomorphism satisfies the universal property of ker.

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



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

holds:



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

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

Now back to the problem itslef,cokerι in **Ab**, as stated, is $\mathbb{Q}/\mathbb{Z}$. The associated π is $\pi(q) = q + \mathbb{Z}$. And cokerι 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:

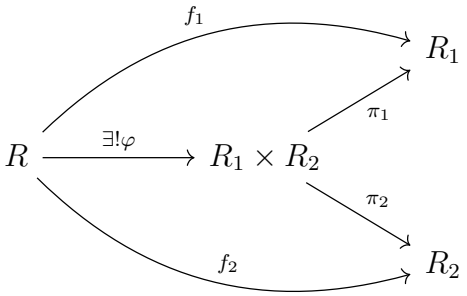
$$j(\frac{p}{q}) = j(pq^{-1}) = j(p)j(q)^{-1} = j(\iota(p))j(\iota(q)) = 0(p)0(q)^{-1} = 0$$

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 cokerι is this object. □

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 π_1, π_2 are ring homomorphisms, we must show that the following diagrams holds:



For (R, f_1, f_2), defines $\varphi : R \to R_1 \times R_2, r \mapsto (f_1(r), f_2(r))$. Then the diagram is commutative. To prove the uniqueness, consider another ring homomorphism $\varphi^{'} : R \to R_1 \times R_2$ 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 $(\mathbb{Z}, +)$.