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 $+, \cdot$ so as to make R^S into a ring, such that R^S is just a copy of R if S is a sigleton.

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,

$$(1+i+j)(2+k) = 1\cdot 2+i\cdot 2+j\cdot 2+1\cdot k+i\cdot k+j\cdot k = 2+2i+2j+kj+i = 2+3i+j+k$$

(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:

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

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

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

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

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

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. □