CS201

Mathematics For Computer Science

Indian Institute of Technology, Kanpur

Group Number: 35

Samarth Varma (180655), Parag Gupta (180500), Satvik Jain (180678)

Assignment 4

Date of Submission: 16/12/2020

Question 1

Let S be a finite set and F be set of all bijections from S to S. Show that F along with the composition operation is a group.

Solution

We need to prove that composition operation satisfies Closure, Associativity, Identity and Inverse Properties.

Let $f : S \to S$ and $g : S \to S$ belongs to F.

- Closure
  - Let $h : S \to S$ be such that $h = f \circ g$. Let $a \in S$ and $b \in S$
  - Let $h(a) = h(b) \implies f \circ g(a) = f \circ g(b)$. which gives $g(a) = g(b)$ as f is one-one.Now since $g(a) = g(b)$,$a = b$ as g is one-one.Hence h is one-one.
  - Let $c \in S$. Then for some $a \in S$, $f(a) = c$. Now $a \in S$ so for some $b \in S$, $g(b) = a$.Hence for every $c \in S$ there exist $b \in S$ such that $h(b) = c$. Hence h is onto.
  - h is one-one and onto and hence $h \in F$. Thus for every f and g in F there is a function $h = f \circ g$ in F.

- Associativity : Since composition is associative for an arbitrary function, it is associative also for the subset of functions given by bijective ones i.e $f \circ (g \circ h) = (f \circ g) \circ h$ for $f, g, h \in F$
- Identity : Let $g \in F$ be such that $g(a) = a$ where $a \in S$. Then for any $f \in F$, $f \circ g(a) = f(a) \implies f \circ g = f$.
- Inverse: $f \in F$ is bijective. Let $g = f^{-1}$ be the inverse. Suppose $b, y \in S$ with $f^{-1}(b) = a = f^{-1}(y)$. Thus $b = f(a) = y$, so f^{-1} is injective. Now suppose $a \in S$ and let $b = f(a)$. Then $f^{-1}(b) = a$. Thus $S = range(f^{-1})$ and so f^{-1} is surjective. Thus $f^{-1} \in F$.

Question 2

Let G be a non-commutative group and $e \in G$ be the identity element. The **order** of an element $g \in G$ denoted as $ord(g)$ is the smallest natural number s such that $g^s = e$ where

$$g^i = \underbrace{g.g.g \ldots g}_{\text{number of } g \text{ is } i}$$

Let a and b be elements of G such that $ord(a) = 7$ and $a^3b = ba^3$. Prove that $ab = ba$.

Solution

Since G is a non-commutative group and $a \in G$, inverse of a exists and is unique.
Since ord$(a) = 7$,

$$a^7 = e$$

$$\implies a^7 = a.a^6 = e$$

Hence a^6 is the inverse of a.
We are given

$$a^3b = ba^3 \tag{2.1}$$

Pre-multiplying 2.1 by a^3

$$a^6b = a^3ba^3 \tag{2.2}$$

Post multiplying 2.1 with a^3

$$a^3ba^3 = ba^6 \tag{2.3}$$

Equating 2.2 and 2.3 to obtain,

$$a^6b = ba^6 \tag{2.4}$$

Pre multiplying and post multiplying 2.4 by a to get-

$$a^7ba = aba^7 \tag{2.5}$$

LHS-

$$a^7 = e \implies a^7ba = eba = ba$$

RHS-

$$a^7 = e \implies aba^7 = abe = ab$$

Equating LHS and RHS to obtain

$$ab = ba$$

Hence Proved

Question 3

Let $\mathbb{Q}[\alpha, \beta]$ denote the smallest subring of $\mathbb{C}$ containing rational numbers $\mathbb{Q}$ and the element $\alpha = \sqrt{2}$ and $\beta = \sqrt{3}$. Let $\gamma = \alpha + \beta$. Is $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$?

Solution

We have been asked whether $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$ From the definition of $\mathbb{Q}[\alpha, \beta]$ we can say that,

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$$

We have also been given that $\sqrt{2}$ and $\sqrt{3}$ are in $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ which is under closed addition,

$$\sqrt{2} + \sqrt{3} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$$

$\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ is a subring of $\mathbb{C}$ that contains $\sqrt{2}+\sqrt{3}$ and $\mathbb{C}$. Since we know that $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$ is the smallest such subring,

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2} + \sqrt{3}]$$

Also,

$$\begin{aligned}(\sqrt{2} + \sqrt{3})^3 &= 2\sqrt{2} + 3\sqrt{3} + 6\sqrt{3} + 9\sqrt{2} \\ &= 11\sqrt{2} + 9\sqrt{3} \\ \implies \sqrt{2} &= \frac{1}{2}((\sqrt{2} + \sqrt{3})^3 - 9(\sqrt{2} + \sqrt{3}))\end{aligned} \tag{3.1}$$

Since $\frac{1}{2} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$ and $\sqrt{2} + \sqrt{3} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$ which is itself closed under addition and multiplication, we can say that $\sqrt{2} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$.

In a similar way from (3.1), $\sqrt{3}$ can be written as,

$$\sqrt{3} = -\frac{1}{2}((\sqrt{2} + \sqrt{3})^3 - 11(\sqrt{2} + \sqrt{3}))$$

and therefore we can say that $\sqrt{3} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$

Thus $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$ is a subring of $\mathbb{Q}$, $\sqrt{2}$, $\sqrt{3}$ and since $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ is the smallest subring, we can conclude that

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2} + \sqrt{3}]$$

But we already know that $\mathbb{Q}[\sqrt{2} + \sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ and now that we got to know that $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Therefore this implies that

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$$

or,

$$\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$$

Where $\alpha = \sqrt{2}, \beta = \sqrt{3}, \gamma = \alpha + \beta$.

Hence Proved

Question 4

An element n of a ring R is called **nilpotent** if there exists $j \in \mathbb{N}$ such that $n^j = 0$. An element u of a ring R is called a **unit** if there exists $v \in R$ such that $uv = 1$. Prove that if $r \in R$ is nilpotent, then $1 - r$ is a unit.

Solution

For a nilpotent element r ($\in R$), there exists $j \in \mathbb{N}$ such that $r^j = 0$. We can use the identity given by

$$\begin{aligned} 1 - r^j &= (1-r)(1 + r + r^2 + r^3 \ldots r^{j-1}) \\ \implies 1 - 0 &= (1-r)(1 + r + r^2 + r^3 \ldots r^{j-1}) \end{aligned}$$

Therefore,

$$\implies (1-r)(1 + r + r^2 + r^3 \ldots r^{j-1}) = 1$$

Let $u = 1 - r$ and $v = 1 + r + r^2 + r^3 \ldots r^{j-1}$.
Since R is closed under addition and multiplication, u and v are in R.

This is of the form $uv = 1$. Hence we can say that $1 - r$ is a unit.

Question 5

Let I and J be ideals of a ring R such that $I + J = R$. Prove that $IJ = I \cap J$ where $IJ = \{xy | x \in I, y \in J\}$.

Solution

First of all, we start by proving that both IJ and $I \cap J$ are ideals.
For $I \cap j$ -
By the definition of an ideal, $I \subseteq R$, $J \subseteq R$.
Hence $I \cap J \subseteq R$.
Now we need to show that $I \cap J$ is closed under addition and multiplication.

- **Closed under addition**
  - Let $x, y \in I \cap J$. Then, $x, y \in I$ and $x, y \in J$.
  - Since I is an ideal and hence closed under addition, $x + y \in I$. similarly, $x + y \in J$.
  - Therefore, $x + y \in I \cap J$.
- **Closed inder multiplication**
  - Let $x \in I \cap J$ and $y \in R$.
  - By definition, $x \in I$ and $x \in J$.
  - Since I is an ideal, the element $x.y \in I$. Similarly, $x.y \in J$.
  - Hence $x.y \in I \cap J$.

  Since $I \cap J$ is closed under addition and multiplication and $I \cap J \subseteq R$, we can conclude that $I \cap J$ is an ideal.

For IJ -

$$IJ = \{\sum_i x_i y_i | x_i \in I, y_i \in J\}$$

Let $x \in I$ and $y \in J$.
Since $y \in J$ and $J \subseteq R$ therefore, $y \in R$.

Since I is an ideal, $xy \in I$ and $I \subseteq R$, therefore $xy \in R$.
Since R is closed under addition,
$\{\sum_i x_i y_i | x_i \in I, y_i \in J\} \ \in R$
This implies that all elements of the set IJ are in R. $\implies IJ \subseteq R$.
Now, we need to show that IJ is closed under addition and multiplication.

- **Closed under addtion**
  - Let $x, y \in IJ$ where $x = \sum_{i=0}^{n} x_i y_i$ and $y = \sum_{i=n+1}^{m+n} x_i y_i$. Here, $x_i \in I$ and $y_i \in J$
  - Clearly, $x + y = \{\sum_{i=0}^{m+n} x_i y_i\} \in IJ$
- **Closed under multiplication**
  - Let $x \in IJ$ and an arbitrary $r \in R$ where $x = \sum_{i=0}^{n} x_i y_i$ for some $x_i \in I$ and $y_i \in J$.
  - We have, $rx = r\sum_{i=0}^{n} x_i y_i = \sum_{i=0}^{n}(rx_i)y_i$
  - The above equality was possible because $x_i \in I$ and I is an ideal which in turn implies that I is associative under multiplication.
  - Since $x_i \in I$ and I is an ideal, $rx_i \in I, r \in R$ by definition.
  - Let $z_i = rx_i \in I$. Then $\{\sum_{i=0}^{n} z_i y_i\} \in IJ$ where $Z_i \in I$ and $y_i \in J$.

Since IJ is closed under addition and multiplication and $IJ \subseteq R$, we can conclude that IJ is an ideal.

Now we know that both IJ and $I \cap J$ are ideals, we can freely compare them.
Here, we will try to prove $IJ \subseteq I \cap J$ and $I \cap J \subseteq IJ$ which in turn would imply $IJ = I \cap J$.

- **Proof that $IJ \subseteq I \cap J$**
  - Let $u \in IJ$ such that $u = \sum_i x_i y_i$ where $x_i \in I$ and $y_i \in J$.
  - $y_i \in J \implies y_i \in R$. Hence $x_i y_i \in I$ by the very definition of an ideal.
  - Since an ideal is closed under addition, we conclude that $u = \sum_i x_i y_i \in I$.
  - The same argument can be applied for the ideal J and shown that $u \in J$.

- Now, $u \in I$ and $u \in J$ implies that $u \in I \cap J$.
- Since u was arbitrary, we conclude that

$$IJ \subseteq I \cap J \tag{5.1}$$

- **Proof that** $I \cap J \subseteq IJ$
  - To prove this part, we assume that the ring is commutative and $1 \in R$.
  - Since $1 \in R$, there exists an $a \in I$ and $b \in J$ such that $a + b = 1$
  - Let some $r \in I \cap J$. It follows that $ar \in IJ$ and $br \in IJ$. Hence $ar + br \in IJ$.
  - Since $a + b = 1$, $r \in IJ$.
  - Now, r was arbitrary in $I \cap J$. Hence

$$I \cap J \subseteq IJ \tag{5.2}$$

Therefore it follows from 5.1 and 5.2 that

$$IJ = I \cap J$$

References