CS201

Mathematics For Computer Science

Indian Institute of Technology, Kanpur

Group Number: 5

Devanshu Singla (190274), Sarthak Rout (190772), Yatharth Goswami (191178)

Assignment 4

Date of Submission: December 16, 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

For proving the above result, we will first provide some standard results for functions.

Lemma 1.1. If $f : X \to Y$, $g : Y \to Z$ and $h : Z \to W$ are functions, then $(h \circ g) \circ f = h \circ (g \circ f)$, where $\circ$ represents the composition operator.

Proof. Note that for every $x \in X$ we have,

$$\begin{aligned}[(h \circ g) \circ f](x) &= (h \circ g)(f(x)) \\ &= h(g(f(x))) \\ &= h((g \circ f)(x)) \\ &= [h \circ (g \circ f)](x)\end{aligned}$$

Therefore, $(h \circ g) \circ f = h \circ (g \circ f)$. □

Lemma 1.2. Suppose $f : X \to Y$ and $g : Y \to Z$ are bijections. Then their composition $h = (g \circ f) : X \to Z$ is also a bijection.

Proof. We will first show that h is injective or we will show that if $h(x) = h(x')$, then we musht have that $x = x'$. Suppose that $h(x) = h(x')$. Using the definition of h this implies that $g(f(x)) = g(f(x'))$. Since, both f and g are injective therefore,

$$\begin{aligned} g(f(x)) = g(f(x')) &\implies f(x) = f(x') \\ &\implies x = x' \end{aligned}$$

Hence, h is injective.
Now, we will show that h is surjective. Since, f and g are both surjections, we have that $f(X) = Y$ and $g(Y) = Z$. Therefore, we have that

$$\begin{aligned} h(A) &= (g \circ f)(A) \\ &= \{z \in Z | (g \circ f)(x) = z, \text{for some } x \in X\} \\ &= \{z \in Z | (g(f(x)) = z, \text{for some } x \in X\} \\ &= \{z \in Z | (g(y) = z, \text{for some } y \in f(X)\} \\ &= g(f(X)) \\ &= g(Y) \\ &= Z \end{aligned}$$

Hence, h is surjective as well and hence h is bijective. □

Lemma 1.3. There exists an inverse for every bijective function $f : X \to Y$ which is also bijective.

Proof. Define $f^{-1} : Y \to X$ by letting $f^{-1}(y)$ be the unique x in X for which $f(x) = y$. (Since, f is surjective there is at least one such x and since f is injective, there is at most one such x. Hence, it is unique). For f^{-1} to be the inverse of f we need to show that for all $x \in X$ and $y \in Y$,

$$f^{-1}(f(x)) = x \text{ and } f(f^{-1}(y)) = y$$

Now, for $x \in X$, we have $f^{-1}(f(x)) = x$ (since $[f^{-1}(f(x))$ is defined to be the element that f sends to $f(x)$). Similarly, for $y \in Y$, $f(f^{-1}(y)) = y$ (since $f^{-1}(y)$ is defined to be the element that f sends to y). Therefore, f^{-1} is an inverse of f.

Now, for proving that f^{-1} is also bijective, we will prove it's injectivity and surjectivity independently. For injectivity, we need to show that if $f^{-1}(y_1) = f^{-1}(y_2)$ then $y_1 = y_2$. Since, $f^{-1}(y_1), f^{-1}(y_2) \in X$, we can fix $x_1, x_2 \in X$ such that, $f^{-1}(y_1) = x_1$ and $f^{-1}(y_2) = x_2$, with the assumption that $x_1 = x_2$. This implies that $f(x_1) = f(x_2)$. Substituting $f^{-1}(y_1) = x_1$ and $f^{-1}(y_2) = x_2$, we can see that

$$
\begin{aligned}
f(f^{-1}(y_1)) &= f(f^{-1}(y_2)) \\
\implies y_1 &= y_2
\end{aligned}
$$

Hence f^{-1} is injective. Now, for proving surjectivity, we need to show that for any arbitrary $x \in X$, we can find a $y \in Y$ such that $f^{-1}(y) = x$. Since, f is bijective, there exists a $z \in X$ such that $f(z) = y$. Therefore, we get $x = f^{-1}(f(z)) = z$. Therefore, we can find for any arbitrary $x \in X$, a $y = f(x) \in Y$ which gets mapped to x by f^{-1}. Hence, we proved the surjectivity and therefore, f^{-1} is bijective. $\square$

Now, to prove that F along with the composition operation is a group, we will check for each of the properties of the group, one by one.

- **Closure:** We need to show that for every $f, g \in F$, there is a unique $h \in F$ such that $f \circ g = h$.

  Proof. We need to show two things here, first is that h is unique and other that $h \in F$. We have with us bijective functions $f : S \to S$ and $g : S \to S$. Note that, domain of h is same as domain of g which is S and at every $s \in S$, $h(s)$ is uniquely defined by $f(g(h))$ and hence h is unique. Now, for proving that $h \in F$, we will use directly **Lemma 1.2**, which gives the result that $h : S \to S$ is a bijection. Hence, closure is satisfied. $\square$

- **Associativity:** We need to prove that for every $f, g, h \in F$, $(h \circ g) \circ f$ = $h \circ (g \circ f)$ which is a direct result of **Lemma 1.1**. Hence, associativity is also satisfied.

- **Identity:** We need to show that there is $I \in F$ such that $f \circ I = f$ for every f.

  Proof. Choose $I : S \to S$ such that $I(s) = s \;\forall\; s \in S$ (identity function). It is trivially a bijective function on S and hence $I \in F$. Also, for every $f \in S$, we have $[f \circ I](s) = f(I(s)) = f(s) \;\forall\; s \in S$ and $[I \circ f](s) = I(f(s)) = f(s) \;\forall\; s \in S$. Hence, the Identity property also gets satisfied. $\square$

- **Inverse:** We need to show that for every $f \in F$, there exists $g \in F$ such that $f \circ g = I$, where I is the identity.

  Proof. In other words we need to show that for all $f \in F$ there exists $g \in F$ such that for all $s \in S$,

  $$[f \circ g](s) = I(s) = s$$

  Using **Lemma 1.3** we know that there exists an inverse for f, say f^{-1} and therefore using the property of inverses $[f \circ f^{-1}](s) = f(f^{-1}(s)) = s \; \forall \; s \in S$ and $[f^{-1} \circ f](s) = f^{-1}(f(s)) = s \; \forall \; s \in S$. Hence, the Inverse property is also satisfied. $\square$

Therefore, F along with composition operation forms a group.

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

$$ord(a) = 7 \implies a^7 = e \text{ (by definition of ord)}$$

$$\begin{aligned}
a^9b &= a^6(a^3b) \\
&= a^6(ba^3) && \text{(given)} \\
&= a^3(a^3b)a^3 && \text{(associative property)} \\
&= a^3(ba^3)a^3 && \text{(given } a^3b = ba^3\text{)} \\
&= (a^3b)a^6 && \text{(associative property)} \\
&= (ba^3)a^6 && \text{(given } a^3b = ba^3\text{)} \\
&= ba^9 \\
\implies a^9b &= ba^9 \\
\implies a^2(a^7)b &= ba^2(a^7) \\
\implies a^2(e)b &= ba^2(e) && (a^7 = e) \\
\implies a^2b &= ba^2 && (ae = a)
\end{aligned}$$

Pre-multiplying both sides by a,

$$\begin{aligned}
a^3b &= aba^2 \\
\implies ba^3 &= aba^2 && \text{(given } a^3b = ba^3\text{)}
\end{aligned}$$

Post-multiplying both sides by a^5,

$$\begin{aligned} ba^8 &= aba^7 \\ \implies ba(a^7) &= ab(a^7) \\ \implies ba(e) &= ab(e) && (a^7 = e) \\ \implies ba &= ab && (ae = e) \end{aligned}$$

Alternative Solution:
We have $a^3b = ba^3$ and $a^7 = e$.
Pre-multiplying the first equation by a^4 and then post-multiplying it by a,

$$a^4a^3ba = a^7ba = ba = a^4ba^4 \implies ba = aa^3ba^4 = a(ba^3)a^4 = aba^3a^4 = aba^7 = ab$$

Hence, $ab = ba$ $\square$.

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

Yes. A subring of a ring $\mathcal{C}$ is a subset of $\mathcal{C}$ that is also a ring in itself under the operations restricted to itself. (Wikipedia)

A ring is closed under addition and multiplication operations. Hence, any linear combination of any rational number along with α, β and $\alpha\beta \in \mathbb{Q}[\alpha, \beta]$. This means $\forall\, x \in \mathbb{Q}[\alpha, \beta]$

$$\exists\, r_1, r_2, r_3, r_4 \in \mathbb{Q} \;\mid\; x = r_1 + r_2 \cdot \alpha + r_3 \cdot \beta + r_4 \cdot \alpha\beta$$

Claim: Let $A = \{x \mid \exists\, a, b, c, r \in \mathbb{Q} \text{ s.t. } x = r + a\alpha + b\beta + c\alpha\beta\}$. Then A with addition operation $(+)$ and multiplication operation $(\times)$ form a ring and this ring is equal to $Q[\alpha, \beta]$.

Proof. For any two elements $x_1, x_2 \in A$ s.t. $x_1 = r_1 + a_1\alpha + b_1\beta + c_1\alpha\beta$ and $x_2 = r_2 + a_2\alpha + b_2\beta + c_2\alpha\beta$,

$$\begin{aligned}
x_1 + x_2 &= (r_1 + a_1\alpha + b_1\beta + c_1\alpha\beta) + (r_2 + a_2\alpha + b_2\beta + c_2\alpha\beta) \\
&= (r_1 + r_2) + (a_1 + a_2)\alpha + (b_1 + b_2)\beta + (c_1 + c_2)\alpha\beta \\
&= r_3 + a_3\alpha + b_3\beta + c_3\alpha\beta
\end{aligned}$$

where, $r_3 = r_1 + r_2, a_3 = a_1 + a_2, b_3 = b_1 + b_2$ and $c_3 = c_1 + c_2$ and $r_3, a_3, b_3, c_3 \in \mathbb{Q}$ by closure property of $\mathbb{Q}$.

Hence, $x_1 + x_2 \in A \implies +$ satisfies closure property in A. Other properties like commutative, associative, additive identity(0) and existence of inverse can be easily seen are satisfied for addition.

$$\begin{aligned}
x_1 x_2 &= (r_1 + a_1\alpha + b_1\beta + c_1\alpha\beta)(r_2 + a_2\alpha + b_2\beta + c_2\alpha\beta) \\
&= (r_1 r_2 + 2a_1 a_2 + 3b_1 b_2 + 6c_1 c_2) + (r_1 a_2 + 3b_1 c_2 + r_2 a_1 + 3b_2 c_1)\alpha \\
&+ (r_1 b_2 + r_2 b_1 + 2a_1 c_2 + 2a_2 c_1)\beta + (r_1 c_2 + r_2 c_1 + a_1 b_2 + a_2 b_1)\alpha\beta \\
&= r_4 + a_4\alpha + b_4\beta + c_4\alpha\beta
\end{aligned}$$

where, $r_4 = (r_1r_2 + 2a_1a_2 + 3b_1b_2 + 6c_1c_2), a_4 = (r_1a_2 + 3b_1c_2 + r_2a_1 + 3b_2c_1), b_4 = (r_1b_2 + r_2b_1 + 2a_1c_2 + 2a_2c_1)$, and $c_4 = (r_1c_2 + r_2c_1 + a_1b_2 + a_2b_1)$ and $r_4, a_4, b_4, c_4 \in \mathbb{Q}$ by closure property of $\mathbb{Q}$

Hence, $x_1x_2 \in A \implies \times$ satisfies closure property in A. Other properties like commutative, associative and multiplicative identity(1) can be easily seen are satisfied for multiplication also. Also, it can be easily seen multiplication is distributive over addition for A.

Hence, A forms a ring with $+$ and $\times$. Since, $A \in \mathbb{C} \implies A$ is subring of $\mathbb{C}$.

Consider $Q[\alpha, \beta]$, since $\alpha, \beta \in Q[\alpha, \beta] \implies \alpha\beta \in Q[\alpha, \beta]$ by closure in multiplication. Also, it implies, $r + a\alpha + b\beta + c\alpha\beta \in Q[\alpha, \beta] \forall r, a, b, c \in \mathbb{Q} \implies A \subseteq Q[\alpha, \beta]$ by closure of addition and multiplication. Hence, every set containing α and β with rational numbers forming subring in $\mathbb{C}$ must contain A as subset and since A forms subring in $\mathbb{C}$, smallest such set is $A \implies Q[\alpha, \beta] = A$. $\square$

If $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$, then, every element in $\mathbb{Q}[\alpha, \beta]$ must be present in $\mathbb{Q}[\gamma]$ and vice-versa.

Lemma: If $y \in \mathbb{Q}[x]$, then $\mathbb{Q}[y] \subseteq \mathbb{Q}[x]$.

Proof: The set of rational numbers $\mathbb{Q}$ is common in both. As $\mathbb{Q}[x]$ is a ring, and $y \in \mathbb{Q}[x]$, hence, $\forall\ z \in \mathbb{Q}[x]$, $y + z$ and $y \cdot z \in \mathbb{Q}[x]$. But, all elements of $\mathbb{Q}[y]$ can be expressed at linear combination of sums and products of rationals and y. So, y and rationals along with their sums and products $\in \mathbb{Q}[x]$, $\mathbb{Q}[y] \subseteq \mathbb{Q}[x]$.

Therefore, if we show that $\gamma \in \mathbb{Q}[\alpha, \beta]$ and simultaneously, α, β and $\alpha\beta \in \mathbb{Q}[\gamma]$, then,

$$\mathbb{Q}[\alpha, \beta] \subseteq \mathbb{Q}[\gamma] \;\&\; \mathbb{Q}[\gamma] \subseteq \mathbb{Q}[\alpha, \beta] \implies \mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$$

The **first part** is obvious as $1 \cdot \alpha + 1 \cdot \beta = \gamma$ by definition, hence, $\gamma \in \mathbb{Q}[\alpha, \beta]$.

For the **second part**, as $\gamma \in \mathbb{Q}[\gamma]$, hence,

$$\gamma \cdot \gamma = \gamma^2 = 5 + 2\sqrt{6} \in \mathbb{Q}[\gamma] \text{ (multiplicative closure)} \implies \sqrt{6} = \alpha\beta \in \mathbb{Q}[\gamma]$$

. Hence, let

$$\delta = \sqrt{6} \cdot \gamma = \sqrt{6}(\sqrt{2} + \sqrt{3}) = \sqrt{12} + \sqrt{18} = 2\sqrt{3} + 3\sqrt{2}$$

. $\delta \in \mathbb{Q}[\gamma]$ due to **multiplicative closure**.

Now,

$$\delta - 2\gamma = \sqrt{2} = \alpha \implies \alpha \in \mathbb{Q}[\gamma]$$

. Also,

$$\beta = \gamma - \alpha \implies \beta \in \mathbb{Q}[\gamma]$$

.

Therefore, as $\gamma \in \mathbb{Q}[\alpha, \beta]$ and α, β and $\alpha\beta \in \mathbb{Q}[\gamma]$, with the ring of rationals $\mathbb{Q}$ common, these two subrings are equal.

Claim: Let A be the same set as in previous claim, then $\mathbb{Q}[\gamma]$ is equal to the subring formed by A in $\mathbb{C}$.

Proof. As $\gamma \in \mathbb{Q}[\gamma]$, hence,

$$\gamma \cdot \gamma = \gamma^2 = 5 + 2\sqrt{6} \in \mathbb{Q}[\gamma] \text{ (multiplicative closure)} \implies \sqrt{6} = \alpha\beta \in \mathbb{Q}[\gamma]$$

. Hence, let

$$\delta = \sqrt{6} \cdot \gamma = \sqrt{6}(\sqrt{2} + \sqrt{3}) = \sqrt{12} + \sqrt{18} = 2\sqrt{3} + 3\sqrt{2}$$

$Since, \delta \in \mathbb{Q}[\gamma]$ due to **multiplicative closure**.

Now,

$$\delta - 2\gamma = \sqrt{2} = \alpha \implies \alpha \in \mathbb{Q}[\gamma]$$

. Also,

$$\beta = \gamma - \alpha \implies \beta \in \mathbb{Q}[\gamma]$$

.

Since, α, β and $\alpha\beta \in \mathbb{Q}[\gamma]$, it implies their linear combination with rational numbers must also belong to $\mathbb{Q}[\gamma]$,

$$\implies A \subseteq \mathbb{Q}[\gamma] \text{ (by definition of } A)$$

Since, A contains γ and rational numbers, and also every ring containing γ and rational numbers must have A as subset, hence minimal such ring containing γ and rational numbers is ring formed by A,

$$\implies Q[\gamma] = A$$

□

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

Since r is nilpotent, there exists $j \in \mathbb{N}$ such that $r^j = 0$. Suppose that $r^m = 0$ for some $m \in \mathbb{N}$.
Observation 1: $\forall\, n \in \mathbb{N}$ and $\forall\, r \in R\; r^n \in R$.

Proof. We will show this by induction on n. For $n = 1$, this is trivially true. Suppose that $r^{n-1} \in R$. Since, $r^n = r^{n-1} \cdot r$ and R is closed under $(\cdot)$, therefore $r^n \in R$. Hence, proved. □

Observation 2: For any $r \in R$ and for all $n \in \mathbf{W}$, $\sum_{i=0}^{i=n} r^i \in R$.

Proof. We will show this by induction on n. For $n = 0$, this is trivially true. Suppose it is true for $n - 1$. Since, $\sum_{i=0}^{i=n} r^i = \sum_{i=0}^{i=n-1} r^i + r^n$ therefore using the above observation that $r^n \in R$ and the fact that $(R, +)$ form a commutative group (which implies that R is closed under $+$), we get that $\sum_{i=0}^{i=n} r^i \in R$. Hence, proved. □

Also, observe that $(R, +)$ forming a commutative group implies that $\sum_{i=1}^{i=n} r_i$ can be permuted in any order to give the same result.

Now, if we take $u = 1 - r \in R$ and $v = \sum_{i=1}^{i=m-1} r^i$. Using the above observations, we know that $v \in R$. Therefore we see that,

$$\begin{aligned} uv &= (1 - r)(1 + r + r^2 + \cdots + r^{m-1}) \\ &= (1 + r + r^2 + \cdots + r^{m-1}) + (-r + (-r^2) + \cdots + (-r^m)) \\ &= (1 + (-r^m)) \text{ \{Using commutativity\}} \\ &= 1 \text{ \{Using nilpotency\}} \end{aligned}$$

Hence, we proved that there exists a v for any arbitrary $u = 1 - r$, such that $uv = 1$ or $1 - r$ 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 $IJ = \{\sum xy | x \in I, y \in J\}$.

Solution

By definition of ideal: If $x \in I \subseteq R$ and I is an ideal, then $r \cdot x \in I \; \forall \, r \in R$.
Also according to Wikipedia, "when R is a commutative ring, the definitions of left, right, and two-sided ideal coincide, and the term ideal is used alone." Hence, it is assumed that this ring is commutative.
For any element $v \in IJ$, we can write $v = \sum\limits_k x_k y_k$ such that $x_k \in I, y_k \in J$. But, $I, J \subseteq R$. As $y_k \in J \subseteq R$, $y \in R$, hence, $x_k y_k \in I$. Similarly, as $x_k \in I \subseteq R$, $x_k \in R$, and $x_k y_k \in J$. As $x_k y_k \in I$ and $x_k y_k \in J$, $x_k y_k \in I \cap J$.
As this is valid for any k and $I \cap J$ is a ring, hence, $v \in I \cap J$. Therefore, for any $v \in IJ, v \in I \cap J \implies \mathbf{IJ \subseteq I \cap J}$.

Consider an element $t \in I \cap J$. As $t \in I \cap J$, $t \in I$ and $t \in J$. Also, $t = 1 \cdot t$ where $1 \in R$ is the multiplicative identity element.
As $I + J = R$, we can write $1 = u + v$ where $u \in I$ and $v \in J$.

$$\implies t = 1 \cdot t = (u + v) \cdot t = u \cdot t + v \cdot t$$

But, $u \in I$ and $t \in J$. Hence, $u \cdot t \in IJ$ and similarly, as $v \in J$ and $t \in I \implies v \cdot t \in IJ$.
Therefore, their sum $u \cdot t + v \cdot t = t \in IJ$ (as IJ is also a ring) for any $t \in I \cap J$ which implies $\mathbf{I \cap J \subseteq IJ}$.
As $IJ \subseteq I \cap J$ and $I \cap J \subseteq IJ$, $\mathbf{IJ = I \cap J}$.