CS201A: ENDSEM

Harshit Bansal(200428), Jaya Gupta(200471), Pratyush Gupta(200717)

March 31, 2022

1. **Answer to question 1:**
   We are given a set U to be set of all sets. Let S be set of all the chains of U defined under partial ordering by inclusion such that $A \leq B$ implies $A \subseteq B$ for $A, B \in U$. Now we define B such that $B = \cup_{i \geq 1} A_i$ which is upper bound of chain C. Now in question it is shown that since every chain has an upper bound, hence by Zorn's lemma set U will have an maximal element say M. But here we cannot apply Zorn's lemma as we see now.
   Let's assume Zorn's lemma holds in this case. This implies that S must also have a maximal element say L and this maximal element is a chain of U. Now L must have an upper bound in U say l. Its easy to see that $L \subseteq L \cup l$ but L is maximal element in S hence $L = L \cup l$, which means l is in L, hence upper bound of maximal chain is in chain itself. We define an element $e \in U$ not belonging to chain L as $e = \{l, \{l\}\}$ and since $l \subset e$, l clearly cannot be upper bound of L, our assumption that Zorn's lemma holds here is false and hence set U cannot have any maximal element.

2. **Answer to question 2:**
   We have to show that a bipartite graph defined as $H(G, G, E)$ has a perfect matching where

   - $(G, \cdot)$ is a finite group with only one element a_2 such that $a_2 \neq e$ and $a_2^2 = e$
   - Edge (a, b) if $a \neq e$ and $b = a^k$ for some $1 < k \leq s$ where s is the minimum positive integer such that $a^s = e$ or $a = e$ and $b = a_2$.

   Before proceeding with the proof we prove that fact that inverse of every element is unique.
   Let different elements a and b have equal inverse c which means $a \cdot c = e = b \cdot c$. Now $b \cdot (a \cdot c) = b$ and $a \cdot (b \cdot c) = a$ which gives $a = b$. This is contradiction to assumed fact that a and b are different, hence all elements have unique inverse in the group.

   Now we prove the fact that there exists finite $k_i \in N$ for every a_i such that $a_i^{k_i} = e$.
   Observe that group G is a finite group by closure property of group for every k, a_i^k is present in the G. Now since G has finite number of elements and there are infinite values of k, which means values must repeat. Lets say $a_i^p = a_i^q$ with $q > p$ then $k_i = min(q - p)$ for every such p, q.

   So we construct a mapping from G to G such that :

   - e maps to a_2,
   - a_2 maps to e,
   - Now consider for every other a_i:
     Let k_i be such that $a_i^{k_i} = e$

$$a_i^{k_i} = e$$
$$a_i^{k_i-1} \cdot a_i = e$$

which means $a_i^{k_i-1}$ is inverse of a_i. Now we need to show that $a_i^{k_i-1}$ is not equal to a_i or e or a_2. This can be shown easily is we see this

- If $a_i^{k_i-1}$ is equal to a_i which leads to equation $a_i^2 = e$ which is contradiction to the condition given in question that only a_2 has this property.
- Clearly a_2 is inverse of itself and every element has a unique inverse hence $a_i^{k_i-1}$ cannot be equal to a_2.
- Similar argument holds for e as well.

Finally we map a_i with its inverse. This gives us unique image for every a_i and hence perfect matching.

3. **Answer to question 3:**

- **To prove : (a) is an ideal of R**

  $(a) = \{b \cdot a | b \in R\}$

  For $I \subseteq R$ to be ideal of ring $(R, *, +)$ it should satisfy the following
  - For every $g, h \in I$, $g + h \in I$
  - For every $a \in R$ and $g \in I$, $(a * g) \in I$
  - $b_1 \cdot a \in (a), b_2 \cdot a \in (a) \Rightarrow (b_1 + b_2) \cdot a \in (a)$
    $$\forall b_1, b_2 \in R \quad \text{and} \quad (b_1 + b_2) \in R$$
  - $b_1 \cdot a \in (a), b_2 \in R \Rightarrow b_2 \cdot b_1 \cdot a \in (a)$
    $$\forall b_2 \in R, (b_1 \cdot a) \in (a) \quad \text{and} \quad b_2 \cdot b_1 \in R$$

  Hence (a) satisfies all the properties of ideal of ring R

- **To prove: R_p is a ring**

  $R_p = \{\frac{f}{g} | f, g \in R \text{ and } g(P) \neq 0\}$

  #R is quotient ring and Elements of R are equivalence classes .

  For $(R_p, +, *)$ to be a ring (here $(+, *)$ means arithmetic modulo C)
  - R_p is closed under addition (If $a, b \in R_p \Rightarrow$(a+b) $\in R_p$)
    $$\frac{f_1}{g_1} \in R_p \quad \text{and} \quad \frac{f_2}{g_2} \in R_p$$
    $$\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{(f_1 * g_2 + f_2 * g_1)}{g_1 * g_2}$$
    $$\forall \mathrm{g}_1, g_2, f_1, f_2 \in R$$
    $$(g_1 * g_2) \in R, (f_1 * g_2) \in R \text{ and } (f_2 * g_1) \in R \Rightarrow (\mathrm{f}_1 * g_2 + f_2 * g_1) \in R$$
    $$\Rightarrow \frac{(f_1 * g_2 + f_2 * g_1)}{g_1 * g_2} \in R_p$$

- Addition is associative and commutative

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_2}{g_2} + \frac{f_1}{g_1} \qquad (g_1 * g_2 = g_2 * g_1)$$

$$(\frac{f_1}{g_1} + \frac{f_2}{g_2}) + \frac{f_3}{g_3} = \frac{f_1}{g_1} + (\frac{f_2}{g_2} + \frac{f_3}{g_3})$$

- R_p contains an additive identity element, which is [0](elements of [0] are of the form (C) where $(C) = Q(x, y) * C$) such that $\frac{f}{g} + [0] = \frac{f}{g}$
- For every element of $\frac{f}{g} \in R_p$ $\exists \frac{-f}{g} \Rightarrow \frac{f}{g} + \frac{-f}{g} = 0$
- R_p is closed under multiplication (If $a, b \in R_p$ ⇒(a*b) $\in R_p$)

$$\frac{f_1}{g_1} \in R_p \quad \text{and} \quad \frac{f_2}{g_2} \in R_p$$

$$\frac{f_1}{g_1} * \frac{f_2}{g_2} = \frac{f_1 * f_2}{g_1 * g_2} \in R_p \qquad (f_1 * f_2, g_1 * g_2 \in R)$$

- Multiplication is associative and also distributive over addition

$$(\frac{f_1}{g_1} * \frac{f_2}{g_2}) * \frac{f_3}{g_3} = \frac{f_1}{g_1} * (\frac{f_2}{g_2} * \frac{f_3}{g_3})$$

$$\frac{f_1}{g_1} * (\frac{f_2}{g_2} + \frac{f_3}{g_3}) = \frac{(f_1}{g_1} * \frac{f_2}{g_2}) + (\frac{f_1}{g_1} * \frac{f_3}{g_3}))$$

- There exists a multiplicative identity [1] such that $\frac{f}{g} * [1] = \frac{f}{g}$.

This proves that R_p is a ring.

- **I_p is maximal ideal of R_p**

  $I_p = \{\frac{f}{g} | f, g \in R \text{ and } g(P) \neq 0 \text{ and } f(P) = 0\}$

  - Let us assume $\exists$ an ideal J_p such that $I_p \subset J_p$. $\Rightarrow \exists$ an element $\frac{F}{G}$ such that $F(P) \neq 0$ and $G(P) \neq 0$.
  - Now, the element $\frac{F(P)-F}{G} \in I_P$, hence $\frac{F(P)-F}{G} \in J_P$.
  - Since J_P is an ideal, $\frac{F}{G} + \frac{F(P)-F}{G}$ will also lie in the ideal. $\Rightarrow \frac{F(P)}{G} \in J_P$. $F(P)$ is constant, so $\frac{1}{F(P)} \in R_P$. So $\frac{1}{F(P)} * \frac{F(P)}{G} \in J_P$. $\Rightarrow \frac{1}{G} \in J_P$.
  - Consider any $\frac{f}{g} \in R_P$. Since $\frac{G}{g} \in R_P \forall g$ such that $g(P) \neq 0$. Hence $\frac{1}{g} \in J_P \forall$ such g. Also, $f \in R_p$ so $f * \frac{1}{g} = \frac{f}{g} \in J_p$.
  - So $\forall \frac{f}{g} \in R_p, \frac{f}{g} \in J_p \Rightarrow J_p = R_p$.

  This proves that I_p is the maximal ideal of R_p .

- **For point** $P = (1, 0), I_p = (y)$
  $(y) = \{[f] * [y] | [f] \in R_p\}$

  $(y) = \{\frac{f}{g} * y \ \ \forall \ \ \frac{f}{g} \in R_p\}$
  $I_p = \{\frac{f}{g} | f, g \in R \text{ and } g(P) \neq 0 \text{ and } f(P) = 0\}$

  - $P = (1, 0)$, so $f * y = 0 \forall f$, hence $\alpha \in I_P \forall \alpha \in (y)$ hence $(y) \subseteq I_P$

  - Consider any element $\frac{F}{G} \in I_P$. $F = N(x, y) + f(x)$ where $N(x, y)$ contains all the terms with atleast one y and $f(x)$ contains the rest of the terms. $f(x)$ is a polynomial in x.

- Since $\frac{F}{G} \in I_P$, $F(P) = 0$. Because every term in $N(x,y)$ contains a y, $N(P) = 0$. $\Rightarrow$ $f(P) = 0$, so $f(1) = 0$, hence $f(x) = (x-1)h(x)$. $\Rightarrow$ $\frac{f}{G} \in I_P$.

- At P, $x^2 + x \neq 0$, so consider $\frac{(x^2+x)f(x)}{(x^2+x)G} = \frac{(x^3-x)h(x)}{(x^2+x)G}$

- $(x^3 - x)h(x) = h(x) * (x^3 + x * y^2 - x) + h(x) * (-x * y^2) = h(x) * C(x,y) + (-h(x) * x * y^2)$ $\Rightarrow$[(x$^3 - x)h(x)] = [(-h(x) * x * y^2)]$([] denotes equivalence classes) which is further equal to $[y]$*[polynomial in x].

- Hence for any $\frac{F}{G} \in I_p$where $F = N(x,y) + (x-1) * h(x)$, it can be written in the form of $\frac{[y*h(x,y)]}{[G']} = (y)$.

This proves that for point $P = (1,0), I_p = (y)$.

- **For point** $P = (0,1)$ **,** $(x) \subseteq I_p$
  $(x) = \{[f] * [x] | [f] \in R_p\}$

  $(x) = \{\frac{f}{g} * x \quad \forall \quad \frac{f}{g} \in R_p\}$

  $I_p = \{\frac{f}{g} | f, g \in R$ and $g(P) \neq 0$ and $f(P) = 0\}$

  Since $P = (0,1)$, all elements of (x) will lie in I_p.($f * x = 0$ at point $P = (0,1)$)

  Let's consider the term $\frac{(y-1)}{g}$. This is of the form $\frac{f}{g}$ such that $f(P) = 0$. So $\frac{(y-1)}{g} \in I_p$ and $\frac{(y-1)}{g} \notin (x)$.

  This clearly proves that $(x) \subseteq I_p$ **and** $(x) \neq I_p$.