I216E: Computational Complexity and Discrete Mathematics

Answers and Comments on Report 3

HOANG, Duc Anh (1520016)

November 24, 2016

Ph.D Student @ Uehara Lab
Japan Advanced Institute of Science and Technology
hoanganhduc@jaist.ac.jp

Problem 1

Let $S = \mathbb{R} \setminus \{-1\}$ and consider an operation defined by $a \circ b = a + b + ab$. Then prove that "$\circ$" is an operation on S. Here, we suppose that arithmetic operations over $\mathbb{R}$ are defined.

Problem 1 (Answer)

It is sufficient to show that if $a, b \in S$ then $a \circ b = a + b + ab \in S$. In other words, we need to show that for $a, b \in \mathbb{R}$, if $a \neq -1$ and $b \neq -1$ then $a \circ b = a + b + ab \neq -1$.

Assume that there are some $a, b \in \mathbb{R}$ with $a \neq -1$, $b \neq -1$ and $a \circ b = a + b + ab = -1$. It follows that $a + b + ab + 1 = (a + 1)(b + 1) = 0$, which implies that either $a = -1$ or $b = -1$, a contradiction.

Problem 2

In the problem 1, prove that $(S, \circ)$ is a group. (Not need to prove "Closure.")

Problem 2 (Answer)

We show that $(S, \circ)$ is a group by definition.

- Close under the operation "$\circ$": see Problem 1.
- Associative: We check that for $a, b, c \in S$, $(a \circ b) \circ c = a \circ (b \circ c)$. Indeed, we have

$$\begin{aligned}(a \circ b) \circ c &= (a + b + ab) \circ c \\ &= (a + b + ab) + c + (a + b + ab)c \\ &= a + b + ab + c + ac + bc + abc \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a \circ (b + c + bc) \\ &= a \circ (b \circ c).\end{aligned}$$

- Identity element: $0 \in S$ is the identity element, since for any $a \in S$,

$$a \circ 0 = 0 \circ a = a + 0 + a.0 = a.$$

- Inverse element: For $a \in S$, $\dfrac{-a}{a+1} \in S$ is the inverse element of a, since

$$a \circ \frac{-a}{a+1} = a - \frac{a}{a+1} - \frac{a^2}{a+1} = 0.$$

Problem 3

Let G be an Abelian group and k be a positive integer. Prove that $G^{(k)} = \{x^k \in G \mid x \in G\}$ is a subgroup of G. Here, you can use $(a \cdot b)^n = a^n \cdot b^n$ for $a, b \in G$ when G is an Abelian group.

Problem 3

Let G be an Abelian group and k be a positive integer. Prove that $G^{(k)} = \{x^k \in G \mid x \in G\}$ is a subgroup of G. Here, you can use $(a \cdot b)^n = a^n \cdot b^n$ for $a, b \in G$ when G is an Abelian group.

Recall that

Theorem 8.3

Let H be a nonempty subset of a group G. Then H is a subgroup of G if and only if H satisfies the following two conditions (1) and (2):

(1) $\forall a, b \in H \Rightarrow a \cdot b \in H$

(2) $\forall a \in H \Rightarrow a^{-1} \in H$

Moreover, two conditions (1) and (2) are equivalent to the following single condition:

(3) $\forall a, b \in H \Rightarrow a \cdot b^{-1} \in H$

Problem 3 (Answer)

We use Theorem 8.3(3) to show that for an Abelian group G and a positive integer k, $G^{(k)} = \{x^k \in G \mid x \in G\}$ is a subgroup of G. That is, we show that for $a, b \in G^{(k)}$, $a \cdot b^{-1} \in G^{(k)}$.

From the definition of $G^{(k)}$, $a = x^k \in G$ and $b = y^k \in G$ for some $x, y \in G$. Our goal is to show that $x^k \cdot (y^k)^{-1} \in G^{(k)}$.

First of all, we prove that $(y^k)^{-1} = (y^{-1})^k$. Let e be the identity element of G. Since $y^k \in G$, $e = y^k \cdot (y^k)^{-1}$. On the other hand, $e = e^k = (y \cdot y^{-1})^k = y^k \cdot (y^{-1})^k$. Therefore, $e = y^k \cdot (y^k)^{-1} = y^k \cdot (y^{-1})^k$, which implies that $(y^k)^{-1} = (y^{-1})^k$ (multiply both sides by $(y^k)^{-1}$ from the left).

Thus, $x^k \cdot (y^k)^{-1} = x^k \cdot (y^{-1})^k = (x \cdot y^{-1})^k$.

Therefore, to show that $x^k \cdot (y^k)^{-1} \in G^{(k)}$, it is sufficient to show $(x \cdot y^{-1})^k \in G^{(k)}$.

- $x \cdot y^{-1} \in G$, because $x, y \in G$.
- $(x \cdot y^{-1})^k \in G$, because $x^k, y^k \in G$ and $(x \cdot y^{-1})^k = x^k \cdot (y^k)^{-1}$.

Problem 4

Prove that the group whose order is a prime number is a cyclic group without proper subgroup.
(Hint: Prove it is a cyclic group, and it does not have a proper subgroup.)

Problem 4 (Answer)

Recall that

Lagrange's Theorem

Let G be a finite group, and H a subgroup of G.Then

(1) $|G| = |G : H||H|$, that is, $|G : H| = |G|/|H|$
(2) Both of order and index of H divide the order of G.

Let G be a group whose order $|G| = p$ for some prime number p. Let e be the identity element of G. Then,

- G is a cyclic group.
  Let $a \neq e$ be any element of G and let $H = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. Then, H is a cyclic subgroup of G. By Lagrange's Theorem, $|H|$ divides $|G| = p$. Since p is a prime number, $|H|$ is either 1 or p. Since $a \neq e$, $|H| \neq 1$, i.e., $|H| = p$. Hence, $H = G$, that is, G is a cyclic group.
- G does not have a proper subgroup.
  Assume that K is a proper subgroup of G, i.e., K is a subgroup that is different from $\{e\}$ and G. By Lagrange's Theorem, $|K|$ divides $|G| = p$. Since p is a prime number, $|K|$ is either 1 or p. That is, K is either $\{e\}$ or G, a contradiction.

Problem 5

Let H be the subgroup of a group G. Prove that H is a normal subgroup, when H has the index 2. (Hint: It is better to divide into $a \in H$ and $a \notin H$.)

Problem 5

Let H be the subgroup of a group G. Prove that H is a normal subgroup, when H has the index 2. (Hint: It is better to divide into $a \in H$ and $a \notin H$.)

Recall that

Normal subgroup

A subgroup N of a group G satisfies the following, N is said to be a normal subgroup of G, and denoted by $G \triangleright N$.

$$aN = Na \ (\forall a \in G).$$

Index

- When G/H is a finite set, so $H \setminus G$ is, and the number of the left and right congruent are equal to each other.
- This number is denoted by $|G : H|$ and called index of H on G.
- When $|G : H| = 2$, we have $G = a_1 H + \cdots + a_n H$.
- Especially, note that $|G : \{e\}| = |G|$, $|G : G| = 1$.

Problem 5 (Answer)

Let H be the subgroup of a group G with $|G : H| = 2$. We prove that H is a normal subgroup by definition, i.e., we show that for every $a \in G$, $aH = Ha$.

- **Case 1:** $a \in H$.
  Since $a \in H$, it follows that $aH = H = Ha$.
- **Case 2:** $a \notin H$.
  Since $|G : H| = 2$, we have $G = H + aH$. It follows that $aH = G \setminus H$. Similarly, $Ha = G \setminus H$. Therefore, $aH = Ha = G \setminus H$.