Solutions
10 November 2020 22:11

Q1.b

1) $G=\langle S, *\rangle$

$b * c = a * c$ ... {given}

$b * c * c^{-1} = a * c * c^{-1}$ ... {c^{-1} exists by definition, post-multiply}

$b * e = a * e$ ... {$aa^{-1} = a^{-1}a = e$, definition of inverse}

$b = a$. ... {$ae = ea = a$, definition of identity}.

$c * b = c * a$ ... {given}

$c^{-1} * c * b = c^{-1} * c * a$ ... {c^{-1} exists by definition, pre-multiply}

$e * b = e * a$. ... {$aa^{-1} = a^{-1}a = e$, definitions of inverse}

$b = a$. ... {$ae = ea = a$, definition of identity}.

$a * b = c * a$ ... {given}

$a^{-1} * a * b = a^{-1} * c * a$ ... {c^{-1} exists by definition, pre-multiply}

$e * b = a^{-1} * c * a$ ... {$aa^{-1} = a^{-1}a = e$, definitions of inverse}

$b = a^{-1} * c * a$ ... {$ae = ea = a$, definition of identity}.

$b = a^{-1} * a * c$ ... {$a * b = b * a$ in an Abelian group}

$b = e * c$ ... {$aa^{-1} = a^{-1}a = e$, definitions of inverse}

$b = c$ ... {$ae = ea = a$, definition of identity}.

2.b) We prove it by induction

Base case: $n=1$, $(a*b)^1 = a * b$ ... {by definition}

Hypothesis: Assume it is true for $n=k$, we shall prove it for $n=k+1$,

$(a*b)^k = a^k * b^k$

$(a*b)^k = (a*b)^k * (a*b) = (a^k * b^k) * (a * b)$

$= (a^k * b^k) * (b * a)$ ... {$a*b = b*a$ in Abelian group}.

$= ((a^k * b^k) * b) * a)$ ... {associative property}.

$= (a^k * b^{k+1} * a)$ ... {associative property}

$= (a^k * a * b^{k+1})$ ... {$a * b = b * a$ in Abelian group}

$= a^{k+1} * b^{k+1}$

2.b)

1.b) $\because 1_G \in H$, $1_G \in K$,

we have $\boxed{1_G \in H \cap K}$ by definition, -(1)

And since, $H \subseteq G$, $K \subseteq G$

we have $\boxed{H \cap K \subseteq G}$. - - (2)

from (1) & (2), we get $H \cap K$ is also a sub-group.

2.4 Assume g is generator of $G = \langle S, * \rangle$.

Say $S = \{1, g, g^2 \ldots g^k\}$

Let $H = \{g^{i_1}, g^{i_2}, \ldots g^{i_p}\}$

such that

$i_1 < i_2 < \ldots < i_p \ldots$ { i_1 is the smallest $\boxed{\text{non-zero}}$ power of g }.

[Note that 1_G may or may not be part of H].

Any number in the series i_k,

$i_k = q \cdot i_1 + r$ .... { by Euclid's Division Algorithm }

$\therefore$ we have

$g^{i_k} = g^{q \cdot i_1} * g^r$

we have

$(g^{q \cdot i_1})^{-1} (g^{i_k}) = (g^{q i_1})^{-1} (g^{q i_1}) * g^r$ .... { premultiply by $(g^{q i_1})^{-1}$, inverse exists in group }

$= e * g^r$ .... { $a * a^{-1} = a^{-1} * a = e$, property of inverse }

$= g^r$ — { $a * e = e * a$, property of identity }

Now, recall from Theorem in class,

that if $h_1 \in H$, $h_2 \in H$,

then $h_1^{-1} h_2 \in H$ for a subgroup.

$\therefore (g^{q i_1}) \in H$, $(g^{i_k}) \in H$

and thus

$(g^{q i_1})^{-1} (g^{i_k}) \in H$

$\therefore$ $g^r \in H$.

$\therefore \quad g^r \in H$

however, since $r < i_1$,

if $r \neq 0$, we have a contradiction that (g^{i_1}) is not the smallest non-zero power of g.

$\therefore \underline{r = 0}$

Thus any element can be written as (g^{i_1})

$$\boxed{g^{i_k} = (g^{i_1})^n} \quad \text{for some } n \in N.$$

Thus it is cyclic & generator is g^{i_1}.

(3)

$$N = \{x \mid x \in G,\ xHx^{-1} = H\}$$

We know that $N \subseteq G$, we only need to show N is a group & that $1_G \in N$.

(1) Closure

if $a \in N, b \in N$,

→ we need to prove

$$a * b \in N$$

or

$$(a * b) * H * (a * b)^{-1} = H.$$

we know

$$(a*b)*H*(a*b)^{-1}$$

$$= (a*b)*H*b^{-1}*a^{-1} \quad \text{--- \{from property derived earlier\}}$$

$$= a*(b*H*b^{-1})*a^{-1} \quad \text{--- \{associativity\}}$$

$$= a*H*a^{-1} \quad \text{--- \{since } b \in N\}$$

$$= H \quad \text{--- \{since } a \in N\}$$

(2) Associative

(2) Associative

We know it is associative as (*) operation is associative.

(3) Identity

Since

$$1_G H (1_G)^{-1} = H,$$

we have identity exists.

(4) Inverse

we have,

$$\text{if } x \in N,$$

then

$$x * H * x^{-1} = H.$$

$\therefore x^{-1} * x * H * x^{-1} = x^{-1} * H$ ... {premultiply by x^{-1}}

$\therefore e * H * x^{-1} = x^{-1} * H$ ... {$\because a^{-1}a = aa^{-1} = e$, property of inverse}

$\therefore H * x^{-1} = x^{-1} * H$ ... {$ae = ea = a$, property of identity}

$\therefore H * x^{-1} * x = x^{-1} * H * x$ ... {post multiply by x}

$\therefore H * e = x^{-1} * H * x$ ... {$aa^{-1} = a^{-1}a = e$, property of inverse}

$\therefore H = x^{-1} * H * x$ ... {$ae = ea = a$, property of identity}

$\therefore$ we have

$$\boxed{x^{-1} * H * x = H}$$

$\therefore x^{-1} \in N.$

$\therefore N$ is a group & since $N \subseteq G$, N is a subgroup

4) → we know that closure is given in the question

if B is finite, list out elements of B as

$$B = \{b_1, b_2, \dots b_m\} \quad \text{{distinct elements}}$$

Take b_i, we take any $(m+1)$ consecutive powers:-

$$b_i, b_i^{i+1}, b_i^{i+2}, \dots b_i^{i+m}$$

Now since $*$ is closed under B,

Now since * is closed under B,
all of the above belong to B,
We can apply PHP here, with the above
elements as pigeons and the set B
as our holes.

$b_1^i, b_1^{i+1}, b_1^{i+2}, \ldots b_1^{i+m}$: Pigeons (m+1)

$B = \{b_1, b_2, \ldots b_m\}$: holes (m)

At least 1 element should be repeated,

$\therefore b_1^i = b_1^j$ with $i<j$.

$\therefore (b_1^i)(b_1^i)^{-1} = b_1^j (b_1)^{-i}$ --- { as inverse exists, we post multiply }

$\therefore e = b_1^{j-i}$ --- {$aa^{-1} = a^{-1}a = e$, property of inverse}

$\therefore \boxed{b_1^{j-1} = e \in B}$

Since $e \in B$, we have $(B, *)$ has identity.

- We know that * is associative as $\langle A, * \rangle$ is a group.
- Now, we just need to prove that inverse exists, and from the above equation, we get that

$$b_1^{j-i} = e$$

and

$$\boxed{b_1(b_1^{j-i-1}) = e}$$

$\therefore (b_1^{j-i-1})$ is the inverse of b_1.

[Similarly, we can show that for any b_k, we must have some $b_k^{\alpha} = b_k^{\beta}$, and that $(b_k^{\beta-\alpha-1})$ would be the inverse] [$\beta > \alpha$].

that $(b_k^{\beta-k-1})$ would be the inverse $[\beta \neq]$.

$\therefore$ $(H, *)$ is a subgroup in this case.

5) Note that here no group is written, due to which we cannot give an example directly.

Assume the opposite, say $H_1 \cup H_2$ is a subgroup.

we take

$a \in H_1 - H_2$

$b \in H_2 - H_1$

from (4)th question, we must have $a * b \in H_1 \cup H_2$,

$\therefore$ $a * b \in H_1 \cup H_2$

then we have

$a * b \in H_1$ or $a * b \in H_2$

→ say if have

$a * b \in H_1$

Then we have,

$b = a^{-1} * (a * b)$

as $a \in H_1$,

$a * b \in H$,

b should be $\in H$

But this contradicts our choice of b.

→ if $a * b \in H_2$,

we take

$a = (a * b) * b^{-1} \in H_2$

we take

$a = (a * b) * b^{-1} \in H_2$.

$\therefore a \in H_2$

which is again a contradiction.

$\therefore$ our assumption was wrong.

[* It can work for 3 groups.]

take $H_1 = \{1, 7\}$

$H_2 = \{1, 11\}$ under the group $\langle Z^*_{12}, X \rangle$

$H_3 = \{1, 5\}$

$H_1 \cup H_2 \cup H_3 = \{1, 5, 7, 11\}$ which is a subgroup. [see below]

3.6

Subsets of the group are created by deleting elements from the group (obviously). This amounts to deleting a row and column from the corresponding Cayley table. Now, you can tell if this new Cayley table represents a group by the following criterion: If each element in the subset appears exactly once in a row and column, then the resulting Cayley table represents a group (more specifically a subgroup of the original group). Stated differently, the rows (and columns) of a Cayley table for a group are simply permutations of the elements of the group.

- this link for theory example.

https://math.stackexchange.com/questions/578200/cayley-tables-and-cyclic-subgroups

(1) $\langle Z^*_{12}, X \rangle$

X	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

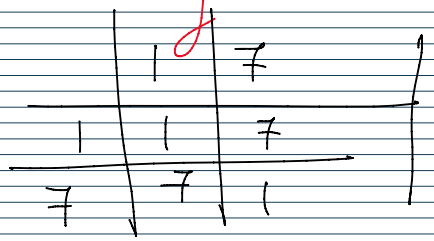
[deleting 1 will never work as 1 should always be part].

deleting 5 →

	1	7	11
1	1	7	11
7	7	1	(5)
11	11	(5)	1

→ because 5 is there, we can't delete 11.

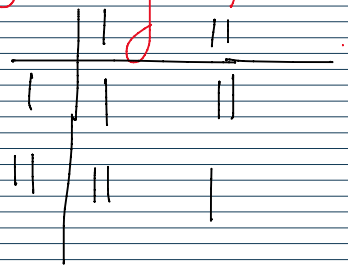
deleting 5, 11 →



works

{1, 7}

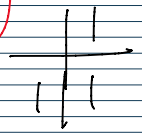
deleting 5, 7 →



works.

{1, 11}

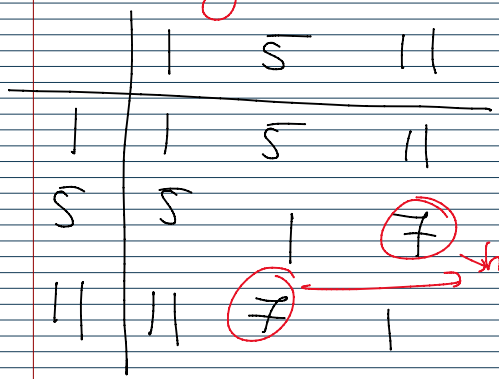
deleting 5, 7, 11 →



works.

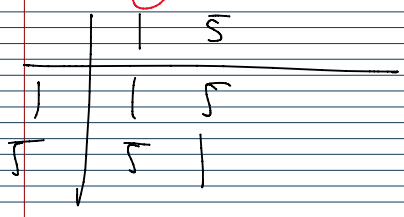
{1}.

deleting 7 →



{1, 5, 11}

deleting 7, 11 →



works

{1, 5}.

check if any case is left out apart from $\{1, 5, 7, 11\}$ itself.

(2) $\langle Z_8^*, \times \rangle$

$$Z_8^* = \{1, 3, 5, 7\}$$

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

→ deleting 3

	1	5	7
1	1	5	7
5	5	1	3
7	7	3	1

→ deleting 3, 5

	1	7
1	1	7
7	7	1

↳ only $\{1, 7\}$

→ deleting 3, 7

	1	5
1	1	5

	1	5
1	1	5
5	5	1

works

{1, 5}

→ delete 3, 5, 7.

	1
1	1

works

{1}

→ delete 5, 7

	1	3
1	1	3
3	3	1

{1, 3}

All cases are covered except {1, 3, 5, 7}.

(3) $\langle \mathbb{Z}_{11}^{\times}, \times \rangle$:

[Alternate method]

take all the primes, and the combination of these primes :→

one prime →

{1, 3, 9, 5, 4}

{1, 2, 4, 8, 5, 10, 9, 5, 4}

[{1, 5, 3, 4, 9} → already done]

{1, 7, 5, 2, 3, 10, 4, 6, 9, 8}

Similarly take 2 primes, 3 primes & 4 primes at a time :-

2 passes

[{1, 2, 3, 4, 5, 6, 7, 8, 9, 10} → done already]

[{1, 2, 5, 10, 6, 5, 7, 8, 9, 4} → done already]

[{1, 2, 7, 3, 10, 9, 8, 4, 6} → done already]

[{1, 3, 9, 5, 4} → done already.]

[{1, 3, 7, 10, 2, 3, 5, 8, 9, 4} → done already.]

{1, 5, 7, 3, 10, 2, 3, 8, 9} → done already

4

3 passes

[{1, 2, 3, 5, 4, 7, 10, 8, 9, 6} → done already]

[{1, 2, 3, 7, 5, 4, 10, 6, 9, 8} → done already]

[{1, 3, 5, 7, 2, 10, 9, 6, 8, 4} → done already}]

[{1, 2, 5, 7, 10, 9, 8, 4, 6, 3} → done already}]

4 passes

[{1, 2, 3, 5, 7, 6, 4, 8, 10, 9} → done already].