MODERN ALGEBRA HW3

18/05/2021

Yosef Goren - 211515606

Gur Telem - 206631848

1. Question

Given G a group and $a, b \in G$.

1.1. Prove $o(ab) = o(ba)$.

Proof. Let's mark $o(ab) = n$ and $o(ba) = m$.
So $(ab)^n = e$ (with n is the minimal number for which it is true).

$$(ba)^{n+1} = b(ab)^n a = bea = (ba) \implies (ba)^{n+1}(ba)^{-1} = (ba)^n = (ba)(ba)^{-1} = e$$

But m is the minimal value for which $(ba)^m = e$ and thus $m \leq n$.
In a completely analog way (replacing $n \Leftrightarrow m$ and $a \Leftrightarrow b$) we get $n \leq m$. Thus $n = m$. $\square$

1.2. Prove $ab = ba \wedge o(b) = m, o(a) = n \wedge (n, m) = 1 \implies o(ab) = o(a)o(b)$.

Proof.

$$a^n = e, b^m = e$$
$$\Downarrow$$
$$e = e \cdot e = e^m e^n = (a^n)^m \cdot (b^m)^n = \cdot (ab)^{mn}$$

Now BWOC let's assume $\exists k < mn : (ab)^k = e$

$$e^m = \left((ab)^k\right)^m = a^{km} \cdot b^{km} = a^{km} \cdot (b^m)^k = a^{km} \cdot e^k = a^{km}$$
$$\Downarrow$$
$$o(a) \mid km$$

Simillarly, $o(b) \mid kn$. So we got $o(b) = m \mid kn \wedge o(a) = n \mid km \implies m \mid k \wedge n \mid k$. And since $(m, n) = 1$ then $mn \mid k$. From the first part, get got $(ab)^{mn} = e \implies k \mid mn$. Thus, $k = mn$. $\square$

2. Question

2.1. Given $m, n \in \mathbb{Z}$ find $m\mathbb{Z} \cap n\mathbb{Z}$.

Proof. Intuition: $m\mathbb{Z}$ is all the numbers that are multiples of m. Like wise $n\mathbb{Z}$ are the multiples of n. So $m\mathbb{Z} \cap n\mathbb{Z}$ are the common multiples. All the common multiples must be a multiple of the lowest common multiple, meaning $m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\,\mathbb{Z}$.

Let's prove it. Let $k \in m\mathbb{Z} \cap n\mathbb{Z}$. So $k \in m\mathbb{Z} \wedge k \in n\mathbb{Z}$. So $\exists t, s \in \mathbb{Z} : mt = ns = k$.

This means that $m \mid k \wedge n \mid k \implies [m, n] \mid k$. So $k \in [m, n]\,\mathbb{Z}$ (from the definition of LCM).

Now let $c \in [m, n]\,\mathbb{Z}$. Meaning $[m, n] \mid c$ but $m \mid [m, n]$ and $n \mid [m, n]$ so $n \mid c$ and $m \mid c$. Thus

$$\exists t, s \in \mathbb{Z} : tn = sm = c \implies c \in m\mathbb{Z} \wedge c \in n\mathbb{Z} \implies c \in m\mathbb{Z} \cap n\mathbb{Z}$$

In conclusion

$$m\mathbb{Z} \cap n\mathbb{Z} \subseteq [m, n]\,\mathbb{Z} \wedge m\mathbb{Z} \cap n\mathbb{Z} \supseteq [m, n]\,\mathbb{Z} \implies m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\,\mathbb{Z}$$

□

2.2. Given G group and $|G| = 15$. Also G has a single subgroup $|H_1| = 3$ and a single $|H_2| = 5$. RTP G is cyclic. In other words $\exists a \in G : \langle a \rangle = 15$.

3. Question

Given the group U_{27}

3.1. **RTP:** $o(2)$ **in** U_{27}**. Is** U_{27} **cyclic?**

Proof. $\langle 2 \rangle = \{1, 2, 4, 8, 16, 5, 10, 20, 13, 26, 25, 23, 19, 11, 22, 17, 7, 7, 14\}$ (from immediete calculations in excel. Also note that $\underset{n}{\operatorname{argmin}}(2^n \mod 27 = 1) = 18$). So $o(2) = 18$.

But from Lagrange theorem, $o(2) = 18 \mid |U_{27}|$. But ofc $|U_{27}| \leq 26$ because there are only 26 elements smaller than 27. It's also known that $o(2) \leq |U_{27}|$ because $\langle 2 \rangle \subseteq U_{27}$. The only multiple of 18 which is between 18 and 27 is 18. so $o(2) = |U_{27}|$. Thus, U_{27} is cyclic. □

3.2. **RTP:** $o(16)$**.**

Proof. Again using excel $\langle 16 \rangle = \{1, 16, 13, 19, 7, 4, 10, 25, 22\}$. Which means that $o(16) = 9$. Also note that

$$\underset{n}{\operatorname{argmin}}(16^n \mod 27 = 1) = 9$$

This also makes sense because $9 \mid 18$ which complies with Lagrange theorem. □

3.3. **RTP:** $0 < a < 27$ **s.t.** $2^{27} \equiv a \pmod{27}$**.**

Proof.

$$2^{27} = 2^{18+9} = 1 \cdot 2^9 = \pmod{27}$$

So for $0 < a = 26 < 27 : 2^{27} \equiv a \pmod{27}$. □

4. Question

Given $G = \mathbb{Z} \oplus \mathbb{Z}$ and $H = 2\mathbb{Z} \oplus 3\mathbb{Z} \subseteq G$ a subgroup.

4.1. **RTP: Is** $(1, 4)\, H = (13, 13)\, H$**.**

Proof. For $6, 3 \in \mathbb{Z}$ we get $(2 \cdot 6, 3 \cdot 3) = (12, 9) \in 2\mathbb{Z} \oplus 3\mathbb{Z}$. So we get $(1, 4) + (12, 9) = (13, 13)$.

Let's look at

$$(12, 9)\, H = (12, 9) \{(2a, 3b) \mid a, b \in \mathbb{Z}\} = \{(12, 9) + (2a, 3b) \mid a, b \in \mathbb{Z}\} = \{(12 + 2a, 9 + 3b) \mid a, b \in \mathbb{Z}\} =$$
$$= \{(2\,(6 + a)\,, 3\,(3 + b)) \mid a, b \in \mathbb{Z}\}$$

But for each $c, d \in \mathbb{Z}$ we can find $a, b \in \mathbb{Z}$ s.t. $6 + a = c \land 3 + b = d$ (and ofc vice versa). And thus

$$\{(2\,(6 + a)\,, 3\,(3 + b)) \mid a, b \in \mathbb{Z}\} = \{(2c, 3d) \mid c, d \in \mathbb{Z}\}$$

So we got that $(12, 9)\, H = H$.

Now let's look at

$$(4, 1)\, H = (4, 1)\,(12, 9)\, H = \{(4, 1) + (12, 9) + (2a, 3b) \mid a, b \in \mathbb{Z}\} = \{(13, 13) + (2a, 3b) \mid a, b \in \mathbb{Z}\} = (13, 13)\, H$$

□

4.2. **Given** $(a, b)\,, (c, d) \in G$**. RTP: Find necessary sufficient condition for** $(a, b)\, H = (c, d)\, H$**.**

Proof. This is super easy $(a, b)\, H = (c, d)\, H \iff (a, b)\, H \subseteq (c, d)\, H \;\; \land \;\; (a, b)\, H \supseteq (c, d)\, H$. DONE!

Now seriously. The necessary sufficient condition would be if $\exists\, (2n, 3m) \in H : (2n, 3m) + (a, b) = (c, d)$. Or in other words $(a - c, b - d) \in H$.

RTP $(a - c, b - d) \in H \iff (a, b)\, H = (c, d)\, H$.

$\Longrightarrow$

Let's assume $(a - c, b - d) \in H$. Similarly to before: let $k, t \in$.

$$(a - c, b - d)\, H = \{(a - c, b - d) + h \mid h \in H\} = \{(a - c, b - d) + (2k, 3l) \mid k, l \in\} = \{(a - c + 2k, b - d + 3l) \mid k, l \in\}$$

But $2 \mid a - c$ because of the assumption and similarly $3 \mid b - d$. Thus $\exists s, t \in$: $a - c = 2s \land b - d = 3t$.

So

$$\{(a - c + 2k, b - d + 3l) \mid k, l \in\} = \{(2s + 2k, 3t + 3l) \mid k, l \in\} = \{(2\,(s + k)\,, 3\,(t + l)) \mid k, l \in\}$$

And like we explained in the previous section, for a constant $m \in$, we can represent each number in as a sum of $n \in$ and m. And each sum is ofc a number in . So this gives us

$$\{(2\,(s + k)\,, 3\,(t + l)) \mid k, l \in\} = \{(2n, 3m) \mid n, m \in\}$$

Thus $(a, b)\, H = (a, b)\,(a - c, b - d)\, H = (c, d)\, H$ like before.

$\Longleftarrow$

Let's assume $(a, b)\, H = (c, d)\, H$.

Let $(k, l) \in \oplus$.

$$(k, l) \in (a, b)\, H \Leftrightarrow (k, l) \in (c, d)\, H$$

$$(k, l) \in (a, b)\, H \Leftrightarrow \exists\, (2n, 3m) \in H : (a, b) + (2n, 3m) = (k, l)$$

And similarly$\exists\, (2s, 3t) \in H : (c, d) + (2s, 3t) = (k, l)$ because of our assumption.

Now we get $(c, d) + (2s, 3t) = (k, l) = (a, b) + (2n, 3m)$ meaning

$$(a - c, b - d) = (2s - 2n, 3t - 3m) = (2\,(s - n)\,, 3\,(t - m)) \in H$$

Because $t - m, s - n \in$.

So we got $(a - c, b - d) \in H$.

This concludes the proof (isn't the first version much nicer?). □

4.3. **RTP: $[G : H]$ and write a representetive for each coset.**

Proof. These are representetives we're going to use $(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)$.

for any other number $(a,b) \in G$, we will be able to find $(2n, 3m) \in H$ s.t. $(a - 2n, b - 3m)$ will equal to one of the above. This is because $a - 2n \mod 2 \in \{0,1\}$ and similarly $b - 3m \mod 3 \in \{0,1,2\}$. Thus, there will be 6 cosets.

$$
\begin{gathered}
(0,0)\,H = \{(0+2a, 0+3b) = (2a, 3b) \mid (2a, 3b) \in H\} = H \\
(0,1)\,H = \{(0+2a, 1+3b) = (2a, 3b+1) \mid (2a, 3b) \in H\} \\
(0,2)\,H = \{(0+2a, 2+3b) = (2a, 3b+2) \mid (2a, 3b) \in H\} \\
(1,0)\,H = \{(1+2a, 0+3b) = (2a+1, 3b) \mid (2a, 3b) \in H\} \\
(1,1)\,H = \{(1+2a, 1+3b) = (2a+1, 3b+1) \mid (2a, 3b) \in H\} \\
(1,2)\,H = \{(1+2a, 2+3b) = (2a+1, 3b+2) \mid (2a, 3b) \in H\}
\end{gathered}
$$

□