MA2202S Homework 2

Qi Ji (A0167793L)

25th September 2018

1

Claim that $(\mu_n, \times) \simeq (\mathbb{Z}/n\mathbb{Z}, +)$. Define $\phi : \mu_n \to \mathbb{Z}/n\mathbb{Z}$, with the knowledge that

$$\mu_n = \left\{ e^{2\pi ik/n} : k \in \{ 0, \dots, n-1 \} \right\}$$

so we can define

$$\phi(z) = \frac{n \log z}{2\pi i}$$

such that ϕ satisfies

$$\phi(e^{2\pi ik/n}) = k.$$

Then we can observe that $\phi^{-1} : \mathbb{Z}/n\mathbb{Z} \to \mu_n$ is given by

$$\phi^{-1}(k) = e^{2\pi ik/n}.$$

Let H be a subgroup of $(\mu_n, \times)$. If H is a trivial subgroup, we are done, so suppose it's not trivial.

Consider $H' = \phi(H)$ the subgroup of $\mathbb{Z}/n\mathbb{Z}$. Let d denote the smallest number in $H' \setminus \{ 0 \}$.

Claim. $d \mid n$ **and** $H' = \{ 0, d, 2d, \dots, n-d \}$ **exactly.** Suppose on the contrary that $d \nmid n$, then there exists $q \in \mathbb{Z}_0^+, r \in \{ 1, \dots, d-1 \}$ such that

$$\begin{aligned} n &= qd + r \\ n - \underbrace{d - d - \cdots - d}_{q \text{ times}} &= r \end{aligned}$$

which implies that $r \in H'$, contradicting minimality of d. So $d \mid n$ which shows that $\{ 0, d, 2d, \dots, n-d \} \subseteq H'$.

For second part of claim, suppose on the contrary we have $H' \supsetneq D = \{ 0, d, 2d, \dots, n-d \}$. We take $k \in H' \setminus D$, then divide k by d, because $k \notin D$, we have $q \in \mathbb{Z}_0^+, r \in \{ 1, \dots, d-1 \}$ such that

$$k = qd + r$$

then by a similar argument as just now, $r \in H'$ which contradicts minimality of d.

Letting $r \in \mathbb{Z}^+$ such that $dr = n$, we have $H' = \{ 0, d, 2d, \dots, (r-1)d \}$, unravel ϕ to get

$$H = \left\{ 1, e^{2\pi id/n}, e^{2\pi i2d/n}, \dots, e^{2\pi i(r-1)d/n} \right\}$$

as $r = n/d$,

$$H = \left\{ 1, e^{2\pi i/r}, e^{2\pi i2/r}, \dots, e^{2\pi i(e-1)/r} \right\}$$

then it can be observed that $H = \mu_r$ with $r \mid n$.

Conversely suppose $H = \mu_r$ where $r \mid n$, let $d \in \mathbb{N}$, $rd = n$. Elements of μ_r can be enumerated as

$$\mu_r = \left\{ 1, e^{2\pi i/r}, e^{2\pi i 2/r}, \dots, e^{2\pi i(r-1)/r} \right\}$$

as $r = n/d$,

$$\mu_r = \left\{ 1, e^{2\pi i d/n}, e^{2\pi i 2d/n}, \dots, e^{2\pi i(r-1)d/n} \right\} \subseteq \mu_n$$

take $e^{2\pi i a d/n}, e^{2\pi i b d/n} \in \mu_r$ where $a, b \in \{ 0, \dots, r-1 \}$, then

$$\begin{aligned} e^{2\pi i a d/n} e^{2\pi i b d/n} &= e^{2\pi i(a+b)d/n} \\ &= e^{2\pi i(a+b-r)d/n} \end{aligned}$$

as $e^{2\pi i r d/n} = e^{2\pi i} = 1$, so in both cases $a + b \geq r$ and $a + b < r$, we have $e^{2\pi i a d/n} e^{2\pi i b d/n} \in \mu_r$, so μ_r is a subgroup.

2

Factors of 15 are $1, 3, 5, 15$. Using question 1, we have trivial subgroups $\{ 0 \}$ and $\langle 1 \rangle = \mathbb{Z}/15\mathbb{Z}$, we also have the non-trivial subgroups $\langle 3 \rangle$ and $\langle 5 \rangle$.

3

i. $H = \mathrm{Stab}_G(s_0)$ is a subgroup of G.

Take $h_1, h_2 \in H$, then

$$\begin{aligned} \pi(h_1 h_2, s_0) &= \pi(h_1, \pi(h_2, s_0)) \\ &= \pi(h_1, s_0) \\ &= s_0 \end{aligned}$$

so $h_1 h_2 \in H$.

Also let $h \in H$,

$$\begin{aligned} s_0 &= \pi(e, s_0) \\ &= \pi(h^{-1}h, s_0) \\ &= \pi(h^{-1}, \pi(h, s_0)) \\ &= \pi(h^{-1}, s_0) \end{aligned}$$

then $h^{-1} \in H$. Therefore H is a subgroup.

ii.

> $\pi(g_1, s_0) = \pi(g_2, s_0)$ if and only if $g_1 \in g_2 H$.

Suppose $\pi(g_1, s_0) = \pi(g_2, s_0)$, then

$$\begin{aligned} \pi(g_2^{-1}, \pi(g_1, s_0)) &= \pi(g_2^{-1}, \pi(g_2, s_0)) \\ \pi(g_2^{-1}g_1, s_0) &= \pi(g_2^{-1}g_2, s_0) \\ &= \pi(e, s_0) \\ &= s_0 \end{aligned}$$

so $g_2^{-1}g_1 \in H$ which implies $g_1 \in g_2 H$.

Conversely suppose $g_1 \in g_2 H$, then $g_2^{-1}g_1 \in H$,

$$\begin{aligned} \pi(g_1, s_0) &= \pi(g_1, \pi(g_1^{-1}g_2, s_0)) \\ &= \pi(g_1, \pi(g_1^{-1}, \pi(g_2, s_0))) \\ &= \pi(g_1 g_1^{-1}, \pi(g_2, s_0)) \\ &= \pi(e, \pi(g_2, s_0)) \\ &= \pi(g_2, s_0) \end{aligned}$$

iii. Show f is well-defined and injective

> where f is defined as
>
> $$\begin{aligned} f : G/H &\to S \\ gH &\mapsto \pi\left(g, s_0\right). \end{aligned}$$

Let $g, g' \in G$,

$$\begin{aligned} & gH = g'H \\ \iff & g \in g'H && \text{by tutorial 3A Q1} \\ \iff & \pi\left(g, s_0\right) = \pi\left(g', s_0\right) && \text{by part ii} \\ \iff & f(gH) = f(g'H) && \text{by definition of } f \end{aligned}$$

the $\Rightarrow$ argument gives well-definedness and the $\Leftarrow$ argument gives injectivity.

iv. $|G| = |O|\,|H|$.

Since G is finite, by theorem 38 we have

$$|G/H| = \frac{|G|}{|H|}.$$

Consider $f' : G/H \to O$ defined by $f'(gH) = f(gH)$, which is just f contracted to its image. As f is already an injection, restricting it to its image will make f' a bijection, then we have

$$\begin{aligned} \frac{|G|}{|H|} &= |G/H| = |O| \\ |G| &= |H|\,|O|. \end{aligned}$$