MAU22101: Group Theory
Assignment 3 due 02/11/2020

Ruaidhrí Campion
19333850
SF Theoretical Physics

I have read and I understand the plagiarism provisions in the General Regulations of the University Calendar for the current year, found at
http://www.tcd.ie/calendar.
I have completed the Online Tutorial in avoiding plagiarism 'Ready, Steady, Write', located at http://tcd-ie.libguides.com/plagiarism/ready-steady-write.

Exercise 1

1.

$$\begin{aligned} m\bar{k} &= 0 \mod m \\ &= [0] \end{aligned}$$

$$\begin{aligned} n\bar{k} &= f([1]) + f([1]) + \ldots + f([1]) \ \ (n \text{ times}) \\ &= f([1] + [1] + \ldots + [1]) \\ &= f([1 + 1 + \ldots + 1]) \\ &= f([n]) \\ &= f([0]) \\ &= [0] \end{aligned}$$

2.

$$\begin{aligned} \text{Bezout's identity} \implies \gcd(m, n) &= am + bn, \ \ a, b \in \mathbb{Z} \\ d &= am + bn \\ d\bar{k} &= am\bar{k} + bn\bar{k} \\ &= a[0] + b[0] \\ &= [0] \end{aligned}$$

3.

$$\begin{aligned} d = 1 \implies \bar{k} &= [0] \\ f([1]) &= [0] \\ cf([1]) &= c[0], \ \ c \in \mathbb{Z} \\ f([c]) &= [0] \end{aligned}$$

All elements in $\mathbb{Z}/n$ are mapped to the identity in $\mathbb{Z}/m \implies \mathbb{Z}/n \longrightarrow 0 \mod m$.

Exercise 2

$$\begin{aligned}
a &= q_0 b + r_0 \\
\implies r_0 &= a - q_0 b \\
\implies \begin{pmatrix} 1 & -q_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} &= \begin{pmatrix} r_0 \\ b \end{pmatrix} \\
\implies \begin{pmatrix} 1 & -q_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & \alpha \\ b & \beta \end{pmatrix} &= \begin{pmatrix} r_0 & \rho_0 \\ b & \beta \end{pmatrix} \\
\text{where } \alpha &= q_0 \beta + \rho_0
\end{aligned}$$

$$\begin{aligned}
T &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\
T^2 &= \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \\
T^3 &= \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \\
&\vdots \\
T^{-1} &= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \\
T^{-2} &= \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} \\
&\vdots \\
T^0 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
T^n &= \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \ \forall\, n \in \mathbb{Z}
\end{aligned}$$

$$\begin{aligned}
\implies T^{-q_0} \begin{pmatrix} a & \alpha \\ b & \beta \end{pmatrix} &= \begin{pmatrix} r_0 & \rho_0 \\ b & \beta \end{pmatrix} \\
&= \begin{pmatrix} a - q_0 b & \alpha - q_0 \beta \\ b & \beta \end{pmatrix}
\end{aligned}$$

This is equivalent to the row operation of (row 1) $-$ q_0(row 2).

$$\begin{aligned}
ST^{-q_0} \begin{pmatrix} a & \alpha \\ b & \beta \end{pmatrix} &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_0 & \rho_0 \\ b & \beta \end{pmatrix} \\
&= \begin{pmatrix} -b & -\beta \\ r_0 & \rho_0 \end{pmatrix}
\end{aligned}$$

We can continue to multiply on the left by T^{-q_i} (and S if the first entry of the resulting matrix is less than the third) until we cannot continue further. This is equivalent to using the Euclidean algorithm until there are no remainders.

$$\begin{aligned}
M &= \begin{pmatrix} 23 & 19 \\ 6 & 5 \end{pmatrix} \\
T^{-3}M &= \begin{pmatrix} 5 & 4 \\ 6 & 5 \end{pmatrix} \\
ST^{-3}M &= \begin{pmatrix} -6 & -5 \\ 5 & 4 \end{pmatrix} \\
T^2ST^{-3}M &= \begin{pmatrix} 4 & 3 \\ 5 & 4 \end{pmatrix} \\
ST^2ST^{-3}M &= \begin{pmatrix} -5 & -4 \\ 4 & 3 \end{pmatrix} \\
T^2ST^2ST^{-3}M &= \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} \\
ST^2ST^2ST^{-3}M &= \begin{pmatrix} -4 & -3 \\ 3 & 2 \end{pmatrix} \\
T^2ST^2ST^2ST^{-3}M &= \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} \\
ST^2ST^2ST^2ST^{-3}M &= \begin{pmatrix} -3 & -2 \\ 2 & 1 \end{pmatrix} \\
T^2ST^2ST^2ST^2ST^{-3}M &= \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \\
ST^2ST^2ST^2ST^2ST^{-3}M &= \begin{pmatrix} -2 & -1 \\ 1 & 0 \end{pmatrix} \\
T^2ST^2ST^2ST^2ST^2ST^{-3}M &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\
&= S \\
\implies M = \begin{pmatrix} 23 & 19 \\ 6 & 5 \end{pmatrix} &= T^3S^{-1}T^{-2}S^{-1}T^{-2}S^{-1}T^{-2}S^{-1}T^{-2}S^{-1}T^{-2}S \\
&= T^3\left(S^{-1}T^{-2}\right)^5 S
\end{aligned}$$

Exercise 3

$$\begin{aligned}
z_1, z_2, z_3 &\in \mathbb{G}_m \\
\text{Associativity: } (z_1 z_2) z_3 &= z_1 (z_2 z_3) && \text{(standard complex multiplication)} \\
\text{Closure: } (z_1 z_2)^N &= {z_1}^N {z_2}^N \\
&= 1 && \implies z_1 z_2 \in \mathbb{G}_m \\
\text{Identity: } 1^N &= 1 && \implies 1 \in \mathbb{G}_m \\
\text{Inverse: } {z_1}^{-1} &= \frac{1}{z_1} \\
&= \frac{z_1^*}{|z_1|^2} && \implies \exists!\ {z_1}^{-1}
\end{aligned}$$

$\implies$ $(\mathbb{G}_m, \times, 1)$ is a group.

We can manually form a map $f : \mathbb{Z}/n \to \mathbb{G}_m$ such that it satisfies the properties of a homomorphism. The properties we must satisfy are the following:

$$\begin{aligned}
f([x] + [y]) &= f([x]) f([y]) \ \forall\ x, y \in \mathbb{Z}/n && f(x * y) = f(x) \circ f(y),\ * = +,\ \circ = \times \\
f([0]) &= 1 && f(1_{\mathbb{Z}/n}) = 1_{\mathbb{G}_m} \\
f([qx]) &= f([x])^q \ \forall\ q \in \mathbb{Z} && [qx] = [x] + [x] + \ldots + [x] \ (q \text{ times})
\end{aligned}$$

$$\begin{aligned}
\text{Label } \bar{k} &= f([1]) \\
f([2]) &= f([(2)(1)]) \\
&= \bar{k}^2 \\
f([3]) &= \bar{k}^3 \\
&\vdots \\
f([n]) &= \bar{k}^n \\
\text{also } f([n]) &= f([0]) \\
&= 1 \\
&= e^{2i\pi} \\
\implies \bar{k} = f([1]) &= e^{\frac{2i\pi}{n}} \\
f([x]) &= e^{\frac{2i\pi}{n} x}
\end{aligned}$$

Say $|N| < n$. Then f would have to map to at least one element in $\mathbb{G}_m$ more than once, and so f would not be injective. Thus, $|N| \geqslant n$. For each $0 \geqslant x \geqslant n - 1$, $f([x])$ will yield a different result, as $e^{ia} = e^{ib} \iff a = 2p\pi b,\ p \in \mathbb{Z}$, and so f is injective. We can check that $f([x]) = e^{\frac{2i\pi}{n} x} \in \mathbb{G}_m$.

$$\begin{aligned}
\left(e^{\frac{2i\pi}{n} x}\right)^N &= \left(e^{2i\pi}\right)^{\frac{Nx}{n}} \\
&= 1^{\frac{Nx}{n}} \\
&= 1 \ \forall\ x, n, N
\end{aligned}$$

We can also double-check the properties that must be satisfied.

$$\begin{aligned} f([x]+[y]) &= f([x+y]) \\ &= e^{\frac{2i\pi}{n}(x+y)} \\ &= e^{\frac{2i\pi}{n}x}e^{\frac{2i\pi}{n}y} \\ &= f([x])f([y]) \\ f([0]) &= e^0 \\ &= 1 \\ f([qx]) &= e^{\frac{2i\pi}{n}qx} \\ &= \left(e^{\frac{2i\pi}{n}x}\right)^q \\ &= f([x])^q \end{aligned}$$

Thus an injective homomorphism $f : \mathbb{Z}/n \longrightarrow \mathbb{G}_m$ can be described by $[x] \longmapsto e^{\frac{2i\pi}{n}x}$, $|N| \geqslant n$.