MTH6106 Group Theory – Coursework 3

November 16, 2023

This coursework counts for 4% of your mark for this module. You should answer all questions, and each question will be marked out of 4. You should give full explanation of your answers. Please submit your solutions on QMPlus by 2pm on Friday 10th November. Your submission must be entirely your own work.

1. Write down the Cayley table for the quotient group $\mathcal{D}_{12}/\langle r^2\rangle$. (You do not need to prove that $\langle r^2\rangle$ is normal.)

   For brevity write $N := \langle r^2\rangle$ and note that $N = \langle r^2\rangle = \{1, r^2, r^4\}$. The right cosets of N are

$$N = \{1, r^2, r^4\}, \qquad N \cdot r = \{r, r^3, r^5\}$$

$$N \cdot s = \{s, r^2 s, r^4 s\}, \qquad N \cdot rs = \{rs, r^3 s, r^5 s\}$$

   and the Cayley table is therefore

	N	$N \cdot r$	$N \cdot s$	$N \cdot rs$
N	N	$N \cdot r$	$N \cdot s$	$N \cdot rs$
$N \cdot r$	$N \cdot r$	N	$N \cdot rs$	$N \cdot s$
$N \cdot s$	$N \cdot s$	$N \cdot rs$	N	$N \cdot r$
$N \cdot rs$	$N \cdot rs$	$N \cdot s$	$N \cdot r$	N

2. Let $d \geq 1$, let $\mathbb{F}$ be a field and let $\mathrm{Aff}_d(\mathbb{F})$ denote the set of all functions $T_{A,v} \colon \mathbb{F}^d \to \mathbb{F}^d$ which have the form $T_{A,v}(x) = Ax + v$, where A is an invertible $d \times d$ matrix with entries in $\mathbb{F}$ and where $v \in \mathbb{F}^d$. Prove that $\mathrm{Aff}_d(\mathbb{F})$ is a group (where the binary operation is given by composition of functions).

   This can be simplified by noticing that $\mathrm{Aff}_d(\mathbb{F})$ is a subset of $\mathrm{Sym}(\mathbb{F}^d)$ and is equipped with the same composition operation, so in particular G2 is satisfied automatically and we only need to check that $\mathrm{Aff}_d(\mathbb{F})$ is closed under composition, contains the identity element of $\mathrm{Sym}(\mathbb{F}^d)$, and contains all inverses. For the first of these three points notice that $(T_{A,v} \circ T_{B,w})(x) = T_{A,v}(T_{B,w}(x)) = T_{A,v}(Bx + w) = ABx + Aw + v = T_{AB,Aw+v}(x)$ for all $x \in \mathbb{F}^d$ and therefore $T_{A,v} \circ T_{B,w} = T_{AB,Aw+v} \in \mathrm{Aff}_d(\mathbb{F})$ as required to prove closure. To see that the identity function belongs to $\mathrm{Aff}_d(\mathbb{F})$ we note that the element $T_{I,0} \in \mathrm{Aff}_d(\mathbb{F})$ satisfies $T_{I,0}(x) = x$ for all $x \in \mathbb{F}^d$ so that $T_{I,0}$ is the identity function. Finally we may check that $(T_{A,v} \circ T_{A^{-1},-A^{-1}v})(x) = A(A^{-1}x - A^{-1}v) + v = x = T_{I,0}(x)$ for all $x \in \mathbb{F}^d$ so that $T_{A,v} \circ T_{A^{-1},-A^{-1}v} = T_{I,0}$ and likewise $T_{A^{-1},-A^{-1}v} \circ T_{A,v} = T_{I,0}$. The inverse function of $T_{A,v}$ is therefore $T_{A^{-1},-A^{-1}v}$ which is an element of $\mathrm{Aff}_d(\mathbb{F})$ as needed.

3. Let $d \geq 1$ and let $\mathbb{F}$ be a field, and define a group of matrices $G \leq \mathrm{GL}_{d+1}(\mathbb{F})$ by
$$G = \left\{ \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix} : A \in \mathrm{GL}_d(\mathbb{F}), v \in \mathbb{F}^d \right\}.$$
Prove that G is isomorphic to the group
$$\mathrm{Aff}_d(\mathbb{F}) = \{T_{A,v} \colon A \in \mathrm{GL}_d(\mathbb{F}), v \in \mathbb{F}^d\}$$
considered in the previous question. (You do not need to prove that G is a group.)

We just need to construct an isomorphism between the two groups: define $\varphi \colon G \to \mathrm{Aff}_d(\mathbb{F})$ by
$$\varphi\left(\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}\right) := T_{A,v}$$
which is clearly surjective by the definition of G. It is also injective: if $T_{A,v} = T_{B,w}$ then $T_{A,v}(x) = T_{B,w}(x)$ for all $x \in \mathbb{F}^d$, so $Ax + v = Bx + w$ for all $x \in \mathbb{F}^d$, so $v = w$ (by taking $x = 0$), so $Ax + v = Bx + v$ for all $x \in \mathbb{F}^d$, so $Ax = Bx$ for all $x \in \mathbb{F}^d$ and therefore $A = B$. Thus
$$\varphi\left(\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} B & w \\ 0 & 1 \end{pmatrix}\right) \implies A = B \text{ and } v = w.$$
To see that it is a homomorphism we note that for every pair of elements of G,
$$\begin{aligned} \varphi\left(\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}\begin{pmatrix} B & w \\ 0 & 1 \end{pmatrix}\right) &= \varphi\left(\begin{pmatrix} AB & Aw+v \\ 0 & 1 \end{pmatrix}\right) \\ &= T_{AB,Aw+v} \\ &= T_{A,v} \circ T_{B,w} \\ &= \varphi\left(\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}\right) \circ \varphi\left(\begin{pmatrix} B & w \\ 0 & 1 \end{pmatrix}\right) \end{aligned}$$
where the equation $T_{AB,Aw+v} = T_{A,v} \circ T_{B,w}$ comes from the answer to the question before.

4. For every integer $r \geq 1$ let $\mathcal{C}_r$ denote the cyclic group
$$\{e^{2\pi ik/r} \colon 0 \leq k < r\} \leq \mathbb{C}^\times.$$

Let $n, n \geq 1$ be a pair of integers whose highest common factor is 1. Define a function $\varphi\colon \mathcal{C}_n \times \mathcal{C}_m \to \mathcal{C}_{nm}$ by

$$\varphi(e^{2\pi ik/n}, e^{2\pi i\ell/m}) := e^{2\pi ik/n} \cdot e^{2\pi i\ell/m}.$$

Prove that φ is an isomorphism.

To see that φ is a homomorphism, let $(e^{2\pi ik/n}, e^{2\pi i\ell/m}), (e^{2\pi ir/n}, e^{2\pi is/m}) \in \mathcal{C}_n \times \mathcal{C}_m$ and note that

$$\begin{aligned}
\varphi((e^{2\pi ik/n}, e^{2\pi i\ell/m}) \cdot (e^{2\pi ir/n}, e^{2\pi is/m})) &= \varphi((e^{2\pi i(k+r)/n}, e^{2\pi i(\ell+s)/m})) \\
&= e^{2\pi i\left(\frac{k+r}{n} + \frac{\ell+s}{m}\right)} \\
&= e^{2\pi i\left(\frac{k}{n} + \frac{\ell}{m}\right)} \cdot e^{2\pi i\left(\frac{r}{n} + \frac{s}{m}\right)} \\
&= \varphi((e^{2\pi ik/n}, e^{2\pi i\ell/m}))\varphi((e^{2\pi ir/n}, e^{2\pi is/m}))
\end{aligned}$$

as required. To demonstrate injectivity it is enough to show that the kernel of φ is trivial. If $\varphi((e^{2\pi ik/n}, e^{2\pi i\ell/m})) = 1$ then $e^{2\pi i(k/n+\ell/m)} = 1$ so $k/n + \ell/m$ must be an integer, call it p. We have $k/n + \ell/m = p$, so $km + n\ell = nmp$, so $n|km$ and $m|n\ell$ by simple rearrangement. Since n and m are coprime it follows that $n|k$ and $m|\ell$; but necessarily $0 \leq k < n$ and $0 \leq \ell < m$, so $k = n = 0$ and the only element of the kernel is $(1, 1)$. This proves injectivity.

To prove surjectivity we would need to show that every $e^{2\pi it/nm} \in \mathcal{C}_{nm}$ is in the image of φ. This means that given any t in the range $0 \leq t < nm$ we must find integers k, ℓ such that $e^{2\pi i(k/n+\ell/m)} = e^{2\pi it/nm}$. This equation holds if and only if $k/n + \ell/m - t/nm$ is an integer, which holds if and only if $km + \ell n = t \mod mn$. Since n is coprime to m there exist integers a, b such that $am + bn = 1$, so $atm + btn = t$ and we can take $k = at \mod n$ and $\ell = bt \mod m$.

However: since both $|\mathcal{C}_n \times \mathcal{C}_m|$ and $|\mathcal{C}_{nm}|$ equal nm, a function from the one set to the other is bijective if and only if it is either injective *or* surjective. It is therefore not necessary to prove *both* injectivity and surjectivity in the detail given above, but instead you can prove only one and deduce bijectivity from $|\mathcal{C}_n \times \mathcal{C}_m| = |\mathcal{C}_{nm}|$.

5. Let $\mathbb{F}$ be a field, and consider the group

$$G := \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{F} \right\} \leq \mathrm{GL}_3(\mathbb{F}).$$

Find the centre $Z(G)$ of the group G. (You do not need to prove that G is a group.)

By definition the matrix

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

belongs to the centre if and only if

$$\begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & d & e\\ 0 & 1 & f\\ 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & d & e\\ 0 & 1 & f\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix}$$

for all $d, e, f \in \mathbb{F}$, if and only if

$$\begin{pmatrix}1 & a+d & b+af+e\\ 0 & 1 & c+f\\ 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & a+d & b+cd+e\\ 0 & 1 & c+f\\ 0 & 0 & 1\end{pmatrix},$$

if and only if $af = cd$ for all $d, f \in \mathbb{F}$, if and only if $a = c = 0$. So

$$Z(G) = \left\{ \begin{pmatrix}1 & 0 & b\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} : b \in \mathbb{F} \right\}.$$

6. Let G and H be groups, and let N be a normal subgroup of G. Decide whether each of the following two statements is true or false. Give a proof or a counterexample in each case.

   (a) The group $G \times H$ is abelian if and only if G and H are both abelian.

   (b) The group G/N is abelian if and only if both G and N are abelian.

   The first statement is true. Note that $G \times H$ is abelian iff for every $(g_1, h_1), (g_2, h_2) \in G \times H$ we have

   $$(g_1, h_1) \cdot (g_2, h_2) = (g_2, h_1) \cdot (g_1, h_1),$$

   iff for every $(g_1, h_1), (g_2, h_2) \in G \times H$ we have

   $$(g_1 g_2, h_1 h_2) = (g_2 g_1, h_2 h_1),$$

   if and only if for every $g_1, g_2 \in G$ and every $h_1, h_2 \in H$,

   $$g_1 g_2 = g_2 g_1 \text{ and } h_1 h_2 = h_2 h_1,$$

   and this last is precisely what it means to say that both G and H are abelian.

   The second statement is false. It is possible to show that if G is abelian then G/N is abelian, but the converse does not hold, making the statement false. Some examples where G/N is abelian and G is not include:

   - $G = S_3$ and $N = \langle (123) \rangle$;
   - $G = Q_8$ and $N = \{1, -1\}$;
   - $G = D_{2n}$ and $N = \{1, r, r^2, \ldots, r^{n-1}\}$, where $n \geq 3$;
   - G any non-abelian group and $N = G'$ the derived subgroup;
   - G any non-abelian group and $N = G$.