Algebra 2 HW1

Gandhar Kulkarni (mmat2304)

1

Assume for the sake of contradiction that there exists an isomorphism $\varphi : \mathbb{C}\backslash\{0\} \to \mathbb{R}\backslash\{0\}$. Then we must have

$$\varphi(i^4) = \varphi(i)^4 = 1.$$

Thus we must have $\varphi(i) = \pm 1$, since $\varphi(i) \in \mathbb{R}\backslash\{0\}$. If $\varphi(i) = 1$, then φ is not one-one. If $\varphi(i) = -1$, then $\varphi(i^2) = -1^2 = 1$, which also means that φ is not one-one. Thus no such isomorphism exists.

2

1. To characterise a linear transformation, it is enough to understand its action on the basis elements, that is $(1,0)^T$ and $(0,1)^T$. Looking at the point on the unit circle that has an angle θ to the x-axis, we can see that it has the coordinate $(\cos\theta, \sin\theta)$. Similarly, we want to see the coordinates of the point that has an angle of $\frac{\pi}{2}+\theta$ to the x-axis. Its coordinates are $(-\sin\theta, \cos\theta)$. Putting it together, we get the required rotation matrix that describes the linear transformation.

2. To confirm that $\varphi : D_{2n} \to GL_2(\mathbb{R})$ is a homomorphism, we need to see that φ respects multiplication, and $\varphi(r)^n = \varphi(s)^2 = I_2$. The latter is easy to check, as

$$\varphi(r)^n = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^n = \begin{pmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{pmatrix} = I_2,$$

and

$$\varphi(s)^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = I_2.$$

Now, is $\varphi(r)\varphi(s) = \varphi(s)\varphi(r)^{-1}$? See that

$$\varphi(r)\varphi(s) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -\sin\theta & \cos\theta \\ \cos\theta & \sin\theta \end{pmatrix}.$$

We can see that

$$\varphi(s)\varphi(r)^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} -\sin\theta & \cos\theta \\ \cos\theta & \sin\theta \end{pmatrix},$$

which means that $\varphi(r)\varphi(s) = \varphi(s)\varphi(r)^{-1}$. Thus we can see that $\varphi(r)$ and $\varphi(s)$ generated D_{2n} in $GL_2(\mathbb{R})$.

3. To check injectivity, we wish to find the kernel of this homomorphism. We know that $\varphi(r^k s^\ell) = \varphi(r)^k \varphi(s)^\ell$. To find the kernel, we say that $\varphi(r^k s^\ell) = \varphi(r)^k \varphi(s)^\ell = I_2$. If $\ell = 1$, then we have

$$\varphi(r)^k \varphi(s) = \begin{pmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -\sin k\theta & -\cos k\theta \\ \cos k\theta & \sin k\theta \end{pmatrix} = I_2.$$

This means that $\cos k\theta = 0 \implies \frac{2k\pi}{n} = \frac{4z\pm 1}{4} 2n\pi$, which means that k cannot be an integer, which is absurd. Thus we must have $\ell = 0$. Then see that

$$\varphi(r)^k = \begin{pmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{pmatrix} = I_2.$$

For this, we already know that n is the smallest possible positive solution, since $\cos\frac{2\pi k}{n} = 1 \implies k = n$. But since we know that $\varphi(r)^n = I_2$, we can pick $k = 0$ as well. Thus we have $\ker\varphi = \{r^0 s^0\}$, that is to say that φ is injective.

3

$$D_{2n} = \left\{ r^i s^j : 0 \le i \le n-1, 0 \le j \le 1, rs = sr^{n-1} \right\}.$$

For any two elements $r^{i_1}s^{j_1}, r^{i_2}s^{j_2} \in D_{2n}$. Let $r^{i_1}s^{j_1} \in Z(D_{2n})$ commute with $r^{i_2}s^{j_2} \in D_{2n}$. Then

$$r^{i_1}s^{j_1} \cdot r^{i_2}s^{j_2} = r^{i_2}s^{j_2} \cdot r^{i_1}s^{j_1}.$$

Working this out, we get

$$r^{n+i_1+(-1)^{j_1}i_2}s^{j_1+j_2} = r^{n+i_2+(-1)^{j_2}i_1}s^{j_2+j_1}.$$

Let $r^{i_2}s^{j_2}$ be arbitrary, then we can divide all cases into the case where $j_1 = 0$ and $j_1 = 1$.

If $j_1 = 1$, then comparing exponents of r on both sides, we have

$$i_1 - i_2 \equiv i_2 + (-1)^{j_2} i_1 \mod n,$$

which means that the answer for i_1 must depend on i_2 and j_2, which means we cannot find an element that commutes with all elements of D_{2n}.

If $j_1 = 0$, then comparing terms we have

$$i_1 - i_2 \equiv i_2 + (-1)^{j_2} i_1 \mod n \implies i_1(1 - (-1)^{j_2}) \equiv 0 \mod n.$$

Then see that the term in brackets could be either 0 or 2, so we need to find i_1 such that the above equation is satisfied only in the case that the term is 2, as in the case of 0 there is no need to check.

1. If n is odd, then we must necessarily have $i_1 | n$ as $2 \nmid n$, implying that $i_1 = 0$. Thus i, the identity rotation is the only element in the centre of D_{2n} for n odd.

2. If n is even, then $2|n$, so we can have that $i_1 | \frac{n}{2}$. Thus we can have $i_1 = 0, \frac{n}{2}$. Thus we see that the centre of D_{2n} for n even is i and r^k, where $k = \frac{n}{2}$.

4

Let $x \in G$ be such that $xZ(G)$ generates $G/Z(G)$. Thus any term in $G/Z(G)$ is of the form $x^a Z(G)$ for some $a \in \mathbb{Z}$. Consider the canonical quotient map $\pi : G \twoheadrightarrow G/Z(G)$ where $\pi(g) = gZ(G)$. Its kernel is $Z(G)$, so we have $G \cong Z(G) \times G/Z(G)$. Thus we can write $g \in G$ as (z, x^a), such that $g = x^a z$. Now take $g_1, g_2 \in G$, and consider $g_1 \cdot g_2 = x^{a_1} z_1 \cdot x^{a_2} z_2 = g_2 = x^{a_1} x^{a_2} z_1 z_2 = g_2 \cdot g_1$, as the order of multiplication of z_1 and z_2 can be switched as it is in the centre. Thus we have G is abelian.

5

Let $n = |G|,$, $|H| = n_1$, and $|N| = n_2$. For an $x \in G$, let k be the smallest positive number such that $x^k \in H$. We can write $n = kq + r$ by the division algorithm. Then see that

$$1 = x^n = x^{kq+r} = (x^k)^q x^r \in H.$$

But since $(x^k)^q \in H$, we must also have $x^r \in H$, which contradicts the minimality of k. Thus $r = 0$, and $k|n$. For some element $x \in H$, let k be that smallest positive integer such that $x^k \in N$. This is guaranteed as H is finite, so k is at most n_1. See that the element $xN \in G/N$ has order k, which just means that the cyclic subgroup of x generated in H has exactly k elements, since $x^k N = eN$. Then we have $|xN| = k | n_1$, and also $k \mid [G : N] = \frac{n}{n_2}$, since as an element of G/N it must divide its order as well. However, since the two are coprime by hypothesis, we must have $k|1$. This means that $x^1 \in N$ for $x \in H$, which implies that $H \le N$, as required.

6

$G = MN$, where $M, N \trianglelefteq G$. Define the map $f : G \to (G/M) \times (G/N)$, where $f(g) = (gM, gN)$. To see that this map is well-defined, see that for $g = g'$ in G, we have $gM = g'M$ and $gN = g'N$ as the canonical projections from G to G/M and G/N are well-defined. From these two maps it can be seen that the map f also respects the group operation, hence this is also a homomorphism. Note that for all $g \in G$, $g = mn$, for $m \in M, n \in N$. Then an arbitrary element of $(G/M) \times (G/N)$ is of the form (nM, mN). Thus we can see that this corresponds to an element $mn \in G$, which can cover all of G. Thus f is surjective. To compute the kernel of f, see that $gM = e_{G/M} \implies g \in M$, and $gN = e_{G/N} \implies g \in N$. Thus $g \in M \cap N$, thus $\ker f = M \cap N$. Using the first isomorphism theorem gives us our result.