Noah Casey

MATH 4720

Homework 4

1 By using Euler's Theorem, show that if $p = 4n + 3$ is a prime integer, there is no solution to the equation $x^2 \equiv -1 \pmod{p}$

We know that p is prime, so for any $x \in \mathbb{Z}$, $\gcd(x, p) = 1$. Thus, we can proceed using Euler's Theorem. For any p prime, the Euler-phi function $\phi(p) = p - 1$, so in this case, $\phi(p) = 4n + 2$. By Euler's theorem, $x^{4n+2} \equiv 1 \pmod{p}$. Now take $x^{4n+3-1} \equiv x^{4n+3}x^{-1} \equiv 1 \pmod{()}p$. Thus, we can write $x^{4n+3} \equiv x \pmod{p}$ by multiplication modulo p Thus, $x = 0$ as $x^p \equiv 0 \pmod{p}$. If $x = 0$ and $4n + 3 \geq 3$, x^2 cannot be congruent to -1 modulo p.

2 Let $\alpha : G \mapsto H$ be a group homomorphism.

a If G is abelian, show that $\alpha(G)$ is an abelian subgroup of G.

Assume G is abelian. Then we know that for any $a, b \in G$, $a + b = b + a$. Now consider $\alpha(a) + \alpha(b)$. As α is a homomorphism, this is $\alpha(a + b)$. G is abelian, so this is $\alpha(b + a) = \alpha(b) + \alpha(a)$, and $\alpha(G)$ is abelian. We now show that this is a subgroup of G. We know that $\alpha(G)$ contains the identity as $\alpha : e_G \mapsto e_{\alpha(G)}$. Furthermore, for any $h = \alpha(g)$, we know that the inverse exists as $\alpha(g^{-1}) = (\alpha(g)^{-1}) = h^{-1}$. Now take some $h_1 = \alpha(g_1)$ and $h_2 = \alpha(g_2)$. Then we show that h_1h_2 is in $\alpha(G)$. Using the properties of homomorphisms, $h_1h_2 = \alpha(g_1)\alpha(g_2) = \alpha(g_1g_2)$, which is clearly in $\alpha(G)$. Thus, $\alpha(G)$ is an abelian subgroup of G.

b Is it possible for $\alpha(G)$ to be non-trivial and abelian if G is non-abelian?

Is there some α such that $\alpha(a) + \alpha(b) = \alpha(b) + \alpha(a)$ when $ab \neq ba$? Assume that we can. Then using the properties of a homomorphism,

$$\alpha(a) + \alpha(b) = \alpha(ab) = \alpha(ba) = \alpha(b) + \alpha(a).$$

However,

$$\begin{aligned} \alpha(ab) &= \alpha(ba) \\ \alpha(ab)\big(\alpha(ba)\big)^{-1} &= id \\ \alpha(ab)\alpha(a^{-1}b^{-1}) &= id \\ \alpha(aba^{-1}b^{-1}) &= id, \end{aligned}$$

which is clearly not true as $aba^{-1}b^{-1} \neq e$, which is necessary in a homomorphism as the identity maps to the identity.

3 Suppose that $G_1 \cong H_1$ and $G_2 \cong H_2$. Show that $G_1 \times G_2 \cong H_1 \times H_2$.

Let $\alpha : G_1 \mapsto H_1$ and $\beta : G_2 \mapsto H_2$ be isomorphisms. Then if $(g_1, g_2) \in G_1 \times G_2$, we must find an isomorphism to $(h_1, h_2) \in H_1 \times H_2$, which will show that these are isomorphic as the points are arbitrary. Let $\varphi : G_1 \times G_2 \mapsto H_1 \times H_2$ be defined as $\varphi(g_1, g_2) = (\alpha(g_1), \beta(g_2)$ for some $(g_1, g_2) \in G_1 \times G_2$.

We first show that φ is a homomorphism. Let $(g_1 g_1^*, g_2 g_2^*) \in G_1 \times G_2$, then using the fact that α and β are isomorphisms,

$$\begin{aligned} \varphi(g_1 g_1^*, g_2 g_2^*) &= \Big(\alpha(g_1 g_1^*), \beta(g_2 g_2^*)\Big) \\ &= \Big(\alpha(g_1)\alpha(g_1^*), \beta(g_2)\beta(g_2^*)\Big) \\ &= \Big(\alpha(g_1), \beta(g_2)\Big)\Big(\alpha(g_1^*), \beta(g_2^*)\Big) \\ &= \varphi(g_1, g_2)\varphi(g_1^*, g_2^*). \end{aligned}$$

We now show that φ is bijective. Let $\varphi(g_1, g_2) = \varphi(g_1^*, g_2^*)$, then $\Big(\alpha(g_1), \beta(g_2)\Big) = \Big(\alpha(g_1^*), \beta(g_2^*)\Big)$. This means that $\alpha(g_1) = \alpha(g_1^*)$ and $\beta(g_2) = \beta(g_2^*)$. As α and

β are isomorphisms, they are injective, so we get that $g_1 = g_1^*$ and $g_2 = g_2^*$ and $(g_1, g_2) = (g_1^*, g_2^*)$. Thus, φ is injective. Now let $(h_1, h_2) \in H_1 \times H_2$. As α and β are surjective, $\alpha(g_1) = h_1$ and $\beta(g_2) = h_2$, so $\Big(\alpha(g_1), \beta(g_2)\Big) = (h_1, h_2)$ and $\varphi(g_1, g_2) = (h_1, h_2)$, so φ is surjective. As φ is a homomorphism and also a bijective map, it is an isomorphism, proving that $G_1 \times G_2 \cong H_1 \times H_2$.

4 Prove that $\mathbb{R}^*$ is not congruent to $\mathbb{C}^*$.

Assume there exists an isomorphism $\varphi : \mathbb{R}^* \mapsto \mathbb{C}^*$. From linear algebra, we know that mappings can be written as matrices, so write $\varphi = A$ such that $\varphi(r) = Ar$. As $\mathbb{R}^*$ is one-dimensional and $\mathbb{C}^*$ is two-dimensional, A is a 2x1 matrix. Recall that matrices only have inverses if they are square; in other words, their dimension must be nxn. Note that A is not square, so it is singular. Thus, it is not a bijective mapping from $\mathbb{R}^* \mapsto \mathbb{C}^*$. Thus, φ has no inverse, and it cannot be an isomorphism. Hence, $\mathbb{R}^*$ is not congruent to $\mathbb{C}^*$.

5 Let T be the subgroup of $GL_2(\mathbb{R})$ consisting of upper-triangular matrices. Let $U = \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) |x \in \mathbb{R}\} \subset T$.

a Show that $U < T$.

We proceed by the first subgroup test. We know that U contains the identity matrix, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Also, for some $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \in U$, we know that its inverse, $\left(\begin{smallmatrix} 1 & -x \\ 0 & 1 \end{smallmatrix}\right) \in U$. Furthermore, for some $A, B \in U$ such that $A = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$, we know that $AB = \left(\begin{smallmatrix} 1 & a+b \\ 0 & 1 \end{smallmatrix}\right)$, which is in U. Hence, $U < T$.

b Prove that U is abelian.

Let $A = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$. Then $AB = \left(\begin{smallmatrix} 1 & a+b \\ 0 & 1 \end{smallmatrix}\right)$. Now take $BA = \left(\begin{smallmatrix} 1 & b+a \\ 0 & 1 \end{smallmatrix}\right)$, but as the entries of matrices in U are in $\mathbb{R}$, $a+b = b+a$ and $\left(\begin{smallmatrix} 1 & a+b \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & b+a \\ 0 & 1 \end{smallmatrix}\right)$. Thus $AB = BA$ and U is abelian.

c Prove that U is normal in T.

By Theorem G22, U is normal if for all $A \in T$, $AUA^{-1} \subset U$. Let $A \in T$ such that $A = \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$, so $A^{-1} = \frac{1}{ac}\left(\begin{smallmatrix} c & -b \\ 0 & a \end{smallmatrix}\right)$ Also let N be an arbitrary element of U such that $U = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$. Then if $ANA^{-1} \in U$, we are done.

$$\begin{aligned}
\frac{1}{ac}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} &= \frac{1}{ac}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} c & -b+na \\ 0 & a \end{pmatrix} \\
&= \frac{1}{ac}\begin{pmatrix} ac & a(-b+na)+ab \\ 0 & ac \end{pmatrix} \\
&= \begin{pmatrix} 1 & \frac{na}{c} \\ 0 & 1 \end{pmatrix} \in U.
\end{aligned}$$

d Show that T/U is abelian.

First, we concretely state what it means for T/U to be abelian. Let A, B be matrices in T. If T/U is abelian, then $(AU)(BU) = (AB)U = (BA)U = (BU)(AU)$. Let $A = \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ and let $B = \left(\begin{smallmatrix} d & e \\ 0 & f \end{smallmatrix}\right)$. Hence, $AB = \left(\begin{smallmatrix} ad & ae+bf \\ 0 & cf \end{smallmatrix}\right)$ and $BA = \left(\begin{smallmatrix} ad & db+ec \\ 0 & cf \end{smallmatrix}\right)$. It must be shown that these lie in the same coset ($(AB)U = (BA)U$) for T/U to be abelian. In fact, these two matrices both lie in the coset of matrices of the form $\left(\begin{smallmatrix} ad & x \\ 0 & cf \end{smallmatrix}\right)$ for $x \in \mathbb{R}$. We know this is a coset as both of these matrices may be found by multiplying $\left(\begin{smallmatrix} ad & 1 \\ 0 & cf \end{smallmatrix}\right)$ by some element in U as all real numbers x are accounted for in the first rows and second columns of the matrices in U. Thus, T/U is abelian.

e Is U normal in $GL_2(\mathbb{R})$?

Set $A \in GL_2(\mathbb{R})$ such that $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ such that $ab - bc \neq 0$. Also set $N \in U$

such that $N = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$. Then

$$\frac{1}{ad-bc}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad-bc}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d-cn & -b+na \\ -c & a \end{pmatrix}$$
$$= \frac{1}{ad-bc}\begin{pmatrix} ad-acn-bc & -ab+a^2n+ab \\ cd-c^2n-cd & -cb+can+ad \end{pmatrix}$$

We stop here as we see that $cd - c^2n - cd = c^2n$, and c^2 nor n is necessarily 0, so the matrix is not necessarily upper triangular, and therefore not necessarily in U. Thus, U is not normal in $GL_2(\mathbb{R})$.

6 Let G be a group. Let $\mathrm{Inn}(G) = \{i_g | g \in G\}$. We know that this is a subgroup of $\mathrm{Aut}(G)$.

a Show that $\alpha : G \mapsto \mathrm{Aut}\, G$ given by $\alpha(g) = i_g$ is a group homomorphism.

Recall that $i_g(x) = gxg^{-1}$. Let $g_1, g_2 \in G$, then using properties of inverses, we see that

$$\begin{aligned}\alpha(g_1)\alpha(g_2)(x) &= i_{g_1} \circ i_{g_2}(x) \\ &= g_1g_2xg_2^{-1}g_1^{-1} \\ &= g_1g_2x(g_1g_2)^{-1} \\ &= i_{g_1g_2} \\ &= \alpha(g_1g_2).\end{aligned}$$

Hence, α is a group homomorphism.

b Justify that $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$.

We first ensure that α is onto $\mathrm{Inn}(G)$. Let i_g be some inner automorphism on G, then $i_g = \alpha(g)$. Thus, $\alpha(G) = \mathrm{Inn}(G)$. By proposition G18, using the fact that G is a subgroup of G and α is a homomorphism, $\alpha(G) < \mathrm{Aut}(G)$. In particular, because α is onto $\mathrm{Inn}(G)$, $\alpha(G) = \mathrm{Inn}(G) < \mathrm{Aut}(G)$.

c Show that $\ker(\alpha) = C(G)$, where $C(G)$ is the center of G.

Letting $id : G \mapsto G$ be the identity mapping. We see that

$$\begin{aligned}\ker(\alpha) &= \{g \in G | i_g = id\} \\ &= \{gxg^{-1} = id(x) | x \in G\}\end{aligned}$$

But recall that $C(G) = \{x \in G | \forall h \in G, gh = hg\}$. Thus, $\ker(\alpha) = \{gxg^{-1} = id(x) | x \in G, g \in C(G)\}$ as if $g \in C(G)$, $gxg^{-1} = xgg^{-1} = xe = x = id(x)$. Hence, $\ker(\alpha) = C(G)$.

d Show that $\mathrm{Inn}(G) \cong G/C(G)$.

Equivalently, we prove that $\mathrm{Inn}(G) \cong G/\ker(\alpha)$. Recall that α is a homomorphism from G to $\mathrm{Aut}(G)$, in particular, α is onto $\mathrm{Inn}(G)$. Let ϕ be the canonical homomorphism from G to $G/\ker(\alpha)$. Thus, there exists an isomorphism $\eta : G/\ker(\alpha) \mapsto \mathrm{Inn}(G)$ by the first isomorphism theorem and $\mathrm{Inn}(G) \cong G/\ker(\alpha) = G/C(G)$ as desired.