Abstract Algebra by Pinter, Chapter 16

Amir Taaki

Abstract

Chapter 16 on Fundamental Homomorphism Theorem

Contents

1 A. Examples of FHT

Use the FHT to prove that the two given groups are isomorphic. Then display their tables.

1.1 Q1

$\mathbb{Z}_5$ and $\mathbb{Z}_{20}/\langle 5\rangle$.

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 \\ 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 \end{pmatrix}$$

$$K = \{0, 5, 10, 15\} = \langle 5\rangle$$

$$f : \mathbb{Z}_{20} \xrightarrow[\langle 5\rangle]{} \mathbb{Z}_5$$

$$\mathbb{Z}_5 \cong \mathbb{Z}_{20}/\langle 5\rangle$$

1.2 Q2

$\mathbb{Z}_3$ and $\mathbb{Z}_6/\langle 3\rangle$.

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$$

$$K = \{0, 3\} = \langle 3\rangle$$

$$f : \mathbb{Z}_6 \xrightarrow[\langle 3\rangle]{} \mathbb{Z}_3$$

$$\mathbb{Z}_3 \cong \mathbb{Z}_6/\langle 3\rangle$$

1.3 Q3

$\mathbb{Z}_2$ and $S_3/\{\epsilon, \beta, \delta\}$.

$$f = \begin{pmatrix} \epsilon & \alpha & \beta & \gamma & \delta & \kappa \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$K = \{\epsilon, \beta, \delta\}$$

$$f : S_3 \underset{\{\epsilon,\beta,\delta\}}{\twoheadrightarrow} \mathbb{Z}_2$$

$$\mathbb{Z}_2 \cong S_3/\{\epsilon, \beta, \delta\}$$

1.4 Q4

From Chapter 3, part C (at the end):

$$P_D = \{A : A \subseteq D\}$$

If A and B are any two sets, their symmetric difference is the set $A + B$ defined as follows:

$$A + B = (A - B) \cup (B - A)$$

$A - B$ represents the set obtained by removing from A all the elements which are in B.

$$P_3 = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

Consider the function $f(C) = C \cap \{a, b\}$

$$P_2 = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$$

The kernel is $\{\varnothing, \{c\}\}$

Using the kernel we create the quotient cosets:

$$\begin{aligned} K &= \{\varnothing, \{c\}\} \\ &= K + \{c\} \\ K + \{a\} &= \{\{a\}, \{a, c\}\} \\ &= K + \{a, c\} \\ K + \{b\} &= \{\{b\}, \{b, c\}\} \\ &= K + \{b, c\} \\ K + \{a, b\} &= \{\{a, b\}, \{a, b, c\}\} \\ &= K + \{a, b, c\} \end{aligned}$$

Applying the function to the cosets, we get:

$$\begin{aligned} f(K) &= \{\varnothing\} \\ f(K \cap \{a\}) &= \{\{a\}\} \\ f(K \cap \{b\}) &= \{\{b\}\} \\ f(K \cap \{a, b\}) &= \{\{a, b\}\} \end{aligned}$$

Thus,

$$f : P_3 \underset{\{\varnothing,\{c\}\}}{\twoheadrightarrow} P_2$$

$$P_2 \cong P_3/\{\varnothing, \{c\}\}$$

1.5 Q5

$\mathbb{Z}_3$ and $(\mathbb{Z}_3 \times \mathbb{Z}_3)/K$ where $K = \{(0,0), (1,1), (2,2)\}$

Consider $f : \mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_3$ by:

$$f(a, b) = a - b$$

$$\mathbb{Z}_3 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2), (2,0), (2,1), (2,2)\}$$

$$\begin{aligned}
\overline{(0,0)} &= K + (0,0) = K + (1,1) = K + (2,2) \\
\overline{(0,1)} &= K + (0,1) = K + (1,2) = K + (2,0) \\
\overline{(0,2)} &= K + (0,2) = K + (1,0) = K + (2,1)
\end{aligned}$$

Applying the function to any element k from the cosets we get:

$$\begin{aligned}
f(0,0) &= f(1,1) = f(2,2) = 0 \\
f(0,1) &= f(1,2) = f(2,0) = 2 \\
f(0,2) &= f(1,0) = f(2,1) = 1
\end{aligned}$$

Thus,

$$f : \mathbb{Z}_3 \times \mathbb{Z}_3 \underset{K}{\twoheadrightarrow} \mathbb{Z}_3$$

$$\mathbb{Z}_3 \cong \mathbb{Z}_3 \times \mathbb{Z}_3/\{(0,0), (1,1), (2,2)\}$$

2 B. Example of the FHT Applied to $F(\mathbb{R})$

2.1 Q1

Let $\alpha : F(\mathbb{R}) \to \mathbb{R}$ be:

$$\alpha(f) = f(1)$$

Let $\beta : F(\mathbb{R}) \to \mathbb{R}$ be:

$$\beta(f) = f(2)$$

Prove α and β are homomorphisms from $F(\mathbb{R})$ onto $\mathbb{R}$.

Let $g, h \in F(\mathbb{R})$, then:

$$
\begin{aligned}
f(g+h) &= (g+h)(1) \\
&= g(1)+h(1)
\end{aligned}
$$

Likewise for β

The functions are onto because the range of each function are $f(1)$ and $f(2)$ respectively.

2.2 Q2

$$
\begin{aligned}
J &= \{f : f(1) = 0, \forall f \in F(\mathbb{R})\} \\
K &= \{f : f(2) = 0, \forall f \in F(\mathbb{R})\}
\end{aligned}
$$

The cosets of $F(\mathbb{R})$ for α are:

$$J + g, \forall g \in F(\mathbb{R})$$

And for β:

$$K + g, \forall g \in F(\mathbb{R})$$

2.3 Q3

For any arbitrary $g, h \in F(\mathbb{R})$ and $k_1, k_2 \in J$,

$$
\begin{aligned}
f((k_1+g)+(k_2+h)) &= (k_1+g+k_2+h)(1) \\
&= f(k_1+g)+f(k_2+h)
\end{aligned}
$$

Thus $J+g$ and $K+g$ are valid quotient groups.

J and K have the same cardinality under $F(\mathbb{R})$ and so:

$$F(\mathbb{R})/J \cong F(\mathbb{R})/K$$

3 C. Example of FHT with Abelian Groups

3.1 Q1

Let $a, b \in G$

$$f(ab) = (ab)^2$$

But G is abelian, so:

$$
\begin{aligned}
(ab)^2 &= a^2b^2 \\
&= f(a)f(b)
\end{aligned}
$$

And $H = \{x^2 : x \in G\}$

So f is a homomorphism of G onto H

3.2 Q2

$ker(f)$ is defined as:

$$K = \{x \in G : f(x) = e\}$$
$$= \{x \in G : x^2 = e\}$$

3.3 Q3

$f : G \to H$ is a homomorphism of G onto H, with a kernel K, $f : G \underset{K}{\twoheadrightarrow} H$ So therefore,

$$H \cong G/K$$

4 D. Group of Inner Automorphisms

See also the videos by Elliot724 on YouTube about automorphisms.

4.1 Q1

For $Aut(G) \subseteq S_G$, prove $Aut(G) \leq S_G$.

We must prove that $Aut(G)$ obeys the group axioms.

Definition of $Aut(G)$:

$$Aut(G) = \{f \in S_G : f(g_1g_2) = f(g_1)f(g_2), \forall g_1, g_2 \in G\}$$

Therefore for any $f_1, f_2 \in Aut(G)$, it is true that:

$$\forall g_1, g_2 \in G, f_1(f_2(g_1g_2)) = f_1(f_2(g_1))f_1(f_2(g_2))$$

Set obeys **closure** property.

Secondly there is an **identity** element $f_e \in S_G$ such that $f_e : g \to g, \forall g \in G$. Thus $f_e \in Aut(G)$.

Lastly $\forall f \in Aut(G), \forall g_1, g_2 \in G$, that there exists:

$$f(\bar{g_1}) = g_1$$
$$f(\bar{g_2}) = g_2$$

Because f is bijective, in particular from the surjective property, we can compose elements in the domain.

$$f(\bar{g_1}\bar{g_2}) = f(\bar{g_1})f(\bar{g_2})$$
$$= g_1g_2$$

Now because know that:

$$f^{-1}(g_1g_2) = f^{-1}(g_1)f^{-1}(g_2)$$

Substituting in the values of g_1 and g_2, we get:

$$f^{-1}(f(\bar{g_1}\bar{g_2})) = f^{-1}(f(\bar{g_1}))f^{-1}(f(\bar{g_2}))$$
$$\bar{g_1}\bar{g_2} = \bar{g_1}\bar{g_2}$$

Thus group has an **inverse**.

$$Aut(G) \leq S_G$$

4.2 Q2

ϕ_a denotes an inner automorphism of G:

$$\text{for every } x \in G \qquad \phi_a(x) = axa^{-1}$$

Prove every inner automorphism is an automorphism of G.

$$\phi_a(x) = axa^{-1}$$

Show homomorphic property:

$$\phi_a(xy) = axya^{-1}$$

But $e = a^{-1}a$, so:

$$\phi_a(xy) = ax(a^{-1}a)ya^{-1} = \phi_a(x)\phi_a(y)$$

So ϕ_a is homomorphic.

Also $\phi_e(x) = x \quad \forall x \in G$

4.3 Q3

Likewise from above:

$$\phi_a \cdot \phi_b = \phi_{ab}$$

Because $a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1}$

For the inverse, we note that:

$$\begin{aligned} \phi_a(x)\phi_b(x) = \phi_e(x) &= x \\ &= (ab)x(ab)^{-1} \end{aligned}$$

It therefore follows that the inverse automorphism of ϕ_a is:

$$(\phi_a)^{-1} = \phi_{a^{-1}}$$

4.4 Q4

$I(G) = \{\phi_a : a \in G\}$. Prove $I(G) \leq Aut(G)$.

Closure: for any $\phi_a, \phi_b \in I(G)$, then $\phi_a \cdot \phi_b \in I(G)$ because $\phi_a \cdot \phi_b = \phi_{ab}$

Identity: ϕ_e is the identity because $eae^{-1} = a$, so $\phi_e \in I(G)$.

Inverses: $\forall \phi_a \in I(G)$, there is an $\phi_{a^{-1}} \in I(G)$ because $\phi_a \cdot \phi_{a^{-1}} = \phi_{aa^{-1}} = \phi_e$, thus $\phi_{a^{-1}} = (\phi_a)^{-1}$

4.5 Q5

$$C = \{a \in G : ax = xa \text{ for every } x \in G\}$$

Let $a \in C$. Then for every $x \in G$:

$$ax = xa \text{ or } axa^{-1} = x$$

4.6 Q6

Let $h : G \to I(G)$ be a function defined by $h(a) = \phi$. Prove that h is a homomorphism from G *onto* $I(G)$ and that C is its kernel.

We can see that $h(ab) = \phi_{ab} = \phi_a \cdot \phi_b = h(a)h(b)$. Lastly the function is surjective (onto) because for every ϕ, there is a corresponding $a \in G$ (possibly multiple if for example the group is abelian), so the mapping is well defined.

The kernel is defined by:

$$K = \{x \in G : f(x) = e\}$$

In our case this is:

$$K = \{a \in G : h(a) = \phi_e\}$$

The center is defined as:

$$C = \{a \in G : axa^{-1} = x \text{ for every } x \in G\}$$

Which is also the same as writing:

$$K = \{a \in G : h(a) = \phi_e\}$$

4.7 Q7

Lastly using the FHT, we note that:

$$h : G \underset{C}{\twoheadrightarrow} I(G)$$

$$I(G) \cong G/C$$

5 E. FHT Applied to Direct Products of Groups

5.1 Q1

Let G and H be groups.

Suppose $J \trianglelefteq G$ and $K \trianglelefteq H$

$$f(x, y) = (Jx, Ky)$$

Assuming $x \in G$ and $y \in H$, then Jx and Ky form the cosets for G and H.

That is for every value from G and H maps onto $(G/J) \times (H/K)$ because:

$$x \in J\bar{x} \iff Jx = J\bar{x}$$
$$y \in K\bar{y} \iff Ky = K\bar{y}$$

$$f : G \times H \to (G/J) \times (H/K)$$

5.2 Q2

$$kerf = \{(x, y) \in G \times H : f(x, y) = (J, K)\} = J \times K$$

5.3 Q3

$$f : G \times H \underset{J \times K}{\twoheadrightarrow} (G/J) \times (H/K)$$

$$(G \times H)/(J \times K) \cong (G/J) \times (H/K)$$

6 F. First Isomorphism Theorem

6.1 Q1

$K \leq G, H \trianglelefteq G$

Both H and K are closed subgroups, so an element in both must by definition remain within $H \cap K$.

Let $h \in H \cap K$, then $\forall x \in G, xax^{-1} \in H$. This also applies to K. Therefore $H \cap K$ is a normal subgroup of K.

6.2 Q2

$HK = \{xy : x \in H \text{ and } y \in K\}$. Prove HK is a subgroup of G.

Let $a, b \in HK$, then $ab = (h_1k_1)(h_2k_2) = h_1(k_1h_2k_1^{-1})k_1k_2$ which is another element in HK.

6.3 Q3

H is a normal subgroup of HK.

Since HK is a subgroup of G then every element of H conjugated with elements from HK also lay within H.

$H \trianglelefteq HK$

6.4 Q4

Let $x \in HK$ then $x = hk$ for some $h \in H, k \in K$. Form the coset $Hx = H(hk) = Hk$.

Thus HK/H may be written as Hk for some $k \in K$.

6.5 Q5

Prove $f(k) = Hk$ is a homomorphism $f : K \to HK/H$, and its kernel is $H \cap K$

Since $Hk_1 = Hk_2$ for k_1, k_2 in the same coset, then any member of the quotient group HK/H is equal to H multiplied by a representative from that member.

To find the kernel, we need every $x \in K$ such that $f(x) = H$, the identity coset. That is $x \in H$. But since we are mapping from K, then $x \in K$ and $x \in H$. In other words, $ker f = H \cap K$.

6.6 Q6

$$f : K \underset{H \cap K}{\twoheadrightarrow} HK/H$$

$$K/(H \cap K) \cong HK/H$$

7 G. Sharper Cayley Theorem

7.1 Q1

To prove ρ_a is a permutation of X, we must show it is a bijective mapping from X to X.

To show it is injective, let $x_1, x_2 \in X$ and $a \in G$. Suppose $\rho_a(x_1H) = \rho_a(x_2H)$. Since $a \in G$ and G is a group, then $a^{-1} \in G$. Then $(ax_1)H = (ax_2)H$ and,

$$x_1H = a^{-1}ax_2H = x_2H$$

Therefore ρ_a is injective.

To show it is surjective, consider $g \in G$ such that $\rho_a(x) = gH$. But we note that $\rho_a(x) = (ax)H$, so:

$$gH = axH \text{ or } xH = a^{-1}gH$$

Thus ρ_a is both injective and surjective and is therefore a bijective mapping from $X \to X$.

7.2 Q2

Prove $h : G \to S_X$ defined by $h(a) = \rho_a$ is a homomorphism.

Definition of ρ_a:

$$\rho_a(xH) = (ax)H$$

Let $a, b \in G$, then $\forall x \in X$:

$$h(ab) = \rho_{ab}$$

$$\rho_{ab}(x) = (abx)H = (a(bxH)) = (\rho_a \cdot \rho_b)(x)$$

Therefore:

$$h(ab) = h(a) \cdot h(b)$$

7.3 Q3

Let ρ_e denote an identity permutation which leaves the coset unchanged.

$$\rho_e(xH) = xH$$

$$h(a) = \rho_a \implies \forall x \in G \qquad \rho_a(xH) = axH = xH$$

But because ρ_a is an identity permutation then $axH = xH$. That is,

$$xax^{-1}H = H$$

Thus the kernel of h is:

$$kerf = \{a \in H : xax^{-1} \in H, \forall x \in G\}$$

7.4 Q4

Since h is a homomorphism by:

$$f : G \underset{kerf}{\twoheadrightarrow} S_x$$

$$G/kerf \cong \bar{S} \leq S_X$$

If group is a normal subgroup then $\forall a \in A$ and $x \in G$, $xax^{-1} \in A$, which is contained in the kernel of f from the last exercise.

If H contains no normal subgroup of G except $\{e\}$ then:

$$kerf = \{e\}$$

So the quotient group $G/ker f$ is simply G, so we have:

$$G \cong \bar{S} \leq S_X$$

Since S_X is a permutation representation, for which we only define permutations depending on the elements in G. This is why the identity is an homomorphism and not an isomorphism.

8 H. Quotient Groups Isomorphic to the Circle Group

8.1 Q1

Cosine and sine identities:

$$\cos(\alpha + \beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$$

$$\sin(\alpha + \beta) = \sin\alpha\cos\beta + \cos\alpha\sin\beta$$

$$\begin{aligned}\operatorname{cis}(x+y) &= (\operatorname{cis} x)(\operatorname{cis} y) \\ &= \cos(x+y) + i\sin(x+y) = (\cos x + i\sin x)(\cos y + i\sin y) \\ &= \cos(x+y) + i\sin(x+y) = \operatorname{cis}(x+y)\end{aligned}$$

8.2 Q2

$$T = \{\operatorname{cis} x : x \in \mathbb{R}\}$$

Properties of a group:

1. Closure
2. Associativity
3. Identity
4. Inverses

Let $u, v \in T$, then the group operation is multiplication and $u = \operatorname{cis} x$ for some $x \in \mathbb{R}$ and $v = \operatorname{cis} y$ for some $y \in \mathbb{R}$.

Then $u \cdot v = (\operatorname{cis} x)(\operatorname{cis} y) = \operatorname{cis}(x+y)$, where $x + y \in \mathbb{R}$ and so $u \cdot v \in T$ which obeys closure property.

Since the result of cis is a complex number, we conclude the group obeys associativity property.

For the identity, we must test whether 1 lies in T. That is $\exists x \in R : \operatorname{cis} x = 1 = \cos x + i\sin x$. Setting $x = 0$, we get $\operatorname{cis} x = 1$, so group obeys identity property.

For inverses, we know 1 lies in the group so:

$$|z| = 1 \implies \frac{1}{|z|} = 1 = |\frac{1}{z}|$$

So the value $\frac{1}{z}$ is also in the unit square.

8.3 Q3

Let $x, y \in \mathbb{R}$

$$\begin{aligned}f(x+y) &= \operatorname{cis}(x+y) \\ &= (\operatorname{cis} x)(\operatorname{cis} y) \\ &= f(x)f(y)\end{aligned}$$

Thus f is a homomorphism $f : \mathbb{R} \to T$

8.4 Q4

$$\begin{aligned}\ker f &= \{x \in \mathbb{R} : f(x) = 1\}\\ &= \{2n\pi : n \in \mathbb{Z}\} = \langle 2\pi \rangle\end{aligned}$$

8.5 Q5

$$f : \mathbb{R} \underset{\langle 2\pi \rangle}{\twoheadrightarrow} T$$

$$T \cong \mathbb{R}/\langle 2\pi \rangle$$

8.6 Q6

$$g(x) = \operatorname{cis} 2\pi x$$

$$\begin{aligned}g(x+y) &= \operatorname{cis}(2\pi x + 2\pi y)\\ &= g(x)g(y)\end{aligned}$$

$\ker g = \mathbb{Z}$ because $\operatorname{cis}(2\pi n) = 1$

8.7 Q7

$$g : \mathbb{R} \underset{\mathbb{Z}}{\twoheadrightarrow} T$$

9 I. Second Isomorphism Theorem

$$H \trianglelefteq G \qquad K \trianglelefteq G \qquad H \subseteq K$$

$$\phi : G/H \to G/K$$

$$\phi(Ha) = Ka$$

9.1 Q1

\$Ha = Hb \$ so $a \in Hb$, hence $a = hb$ for some $h \in H$

$$\phi(Ha) = \phi(Hhb) = \phi(Hb)$$

If $a = he$ then $\phi(Ha) = \phi(H)$ so ϕ has an identity.

9.2 Q2

Because H is a normal subgroup then $Ha = aH$ so $HaHb = Hab$. We can see this by:

$$\begin{aligned}h_1ah_2b &= h_1ah_2a^{-1}ab\\ &= h_1\bar{h}_2ab\end{aligned}$$

$$\begin{aligned}\phi(HaHb) &= \phi(Hab) = Kab\\ &= Kab = KaKb && = \phi(Ha)\phi(Hb)\end{aligned}$$

9.3 Q3

Let there be a Ka, then $\phi(Ha)$ maps to that value. That is for a set Ka, let $x = ka$, then $a = xk^{-1}$. Thus function is surjective.

9.4 Q4

$$K/H = \{He, Ha, Hb, \dots\}$$

$$\begin{aligned} \ker \phi &= \{aH : Ka = K, \forall a \in G\} \\ &= \{aH : a \in K, \forall a \in G\} \end{aligned}$$

But $K \leq G$ so:

$$\ker \phi = \{aH : a \in K\}$$

9.5 Q5

$$\phi : G/H \underset{K/H}{\twoheadrightarrow} G/K$$

$$(G/H)/(K/H) \cong G/K$$

10 Correspondence Theorem

$$f : G \underset{K}{\twoheadrightarrow} H$$

$$S \leq H$$

$$S^* = \{x \in G : f(x) \in S\}$$

10.1 Q1

Prove $S^* \leq G$

Let $x, y \in S^*$, then $f(x) \in S$ and $f(y) \in S$

Since f is a homomorphism then $f(xy) = f(x)f(y) \in S$

So $xy \in S^*$

10.2 Q2

Prove $K \subseteq S^*$

$$K = \{x \in G : f(x) = e_H\}$$

$e_H \in S$ because S is a group.

Thus $K \subseteq S^*$

10.3 Q3

Let g be the restriction of f to S^*. That is, $g(x) = f(x)$ for every $x \in S^*$ and S^* is the domain of g. Prove g is a homomorphism from S^* onto S and $K = \ker g$.

$$S \leq H$$

Let $s \in S$, then $g(x) = S$, but definition of $S^* = \{x : f(x) \in S\}$, thus $x \in S^*$ and g is a homomorphism from S^* onto S.

$K = \ker g$ because $K \subseteq S^*$ and $g(x) = f(x)$

10.4 Q4

$$g : S^* \underset{K}{\twoheadrightarrow} S$$

$$S \cong S^*/K$$