Abstract Algebra by Pinter, Chapter 16

Amir Taaki

Chapter 16 on Fundamental Homomorphism Theorem

Contents

A. Examples of FHT

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

Q1

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

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

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

$$f : \mathbb{Z}_{20} \underset{\langle 5 \rangle}{\twoheadrightarrow} \mathbb{Z}_5$$

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

Q2

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

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

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

$$f : \mathbb{Z}_6 \underset{\langle 3 \rangle}{\twoheadrightarrow} \mathbb{Z}_3$$

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

Q3

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

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

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

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

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

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.

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

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

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

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

Using the kernel we create the quotient cosets:

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

Applying the function to the cosets, we get:

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

Thus,

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

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

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,

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

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

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

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.

Q2

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

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

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

And for β:

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

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:

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

C. Example of FHT with Abelian Groups

Q1

Let $a, b \in G$

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

But G is abelian, so:

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

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

So f is a homomorphism of G onto H

Q2

$ker(f)$ is defined as:

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

Q3

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

$$H \cong G/K$$

D. Group of Inner Automorphisms

See also the videos by Elliot724 on YouTube about automorphisms.

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 $Aut(G)$:

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

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

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

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:

$$\begin{aligned} f(\bar{g_1}) &= g_1 \\ f(\bar{g_2}) &= g_2 \end{aligned}$$

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

$$\begin{aligned} f(\bar{g_1}\bar{g_2}) &= f(\bar{g_1})f(\bar{g_2}) \\ &= g_1 g_2 \end{aligned}$$

Now because know that:

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

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

$$\begin{aligned} f^{-1}(f(\bar{g_1}\bar{g_2})) &= f^{-1}(f(\bar{g_1}))f^{-1}(f(\bar{g_2})) \\ \bar{g_1}\bar{g_2} &= \bar{g_1}\bar{g_2} \end{aligned}$$

Thus group has an **inverse**.

$$Aut(G) \leq S_G$$

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

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:

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

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

Q5

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

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

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

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:

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

Q7

Lastly using the FHT, we note that:

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

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

E. FHT Applied to Direct Products of Groups

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:

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

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

Q2

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

Q3

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

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

F. First Isomorphism Theorem

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.

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.

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.

$H \trianglelefteq HK$

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 $k \in K$.

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, $ker f = H \cap K$.

Q6

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

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

G. Sharper Cayley Theorem

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 $X \to X$.

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:

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

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:

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

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 $G/kerf$ 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.

H. Quotient Groups Isomorphic to the Circle Group

Q1

Cosine and sine identities:

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

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

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

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.

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 $f : \mathbb{R} \to T$

Q4

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

Q5

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

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

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 $\operatorname{cis}(2\pi n) = 1$

Q7

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

I. Second Isomorphism Theorem

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

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

$$\phi(Ha) = Ka$$

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.

Q2

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

$$\begin{aligned} h_1 a h_2 b &= h_1 a h_2 a^{-1} ab \\ &= h_1 \bar{h}_2 ab \end{aligned}$$

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

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.

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:

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

Q5

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

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

Correspondence Theorem

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

$$S \leq H$$

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

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 $xy \in S^*$

Q2

Prove $K \subseteq S^*$

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

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

Thus $K \subseteq S^*$

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 $g(x) = f(x)$

Q4

$$g : S^* \xrightarrow[K]{} S$$

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

K. Cauchy's Theorem

See also proof in this video.

$|G| = k$ and p is a prime divisor. Assume G is not abelian. Let C be the center of G and C_a be the centralizer of a for each $a \in G$.

Let $k = c + k_s + \cdots + k_t$ be the class equation.

Show G has at least one element of order p.

Q1

Prove: if p is a factor of $|C_a|$ for any $a \in G$ where $a \notin C$, we are done.

$$C_a = \{x \in G : xa = ax\}$$

Since C_a is subgroup, then this implies there is an element of order p inside C_a by Lagrange's theorem.

Q2

Prove that for any $a \notin C$ in G, if p is not a factor of $|C_a|$ then p is a factor of $(G : C_a)$.

From orbit-stabilizer theorem, orbits are conjugacy classes and stabilizers are centralizers, considering the group acting on itself through conjugation.

$$O(u) = \{g(u) : g \in G\}$$

$$G_u = \{g \in G : g(u) = u\}$$

$$C_a = \{x \in G : xax^{-1} = a\}$$

$$[a] = \{xax^{-1} : x \in G\}$$

Let the group action $g(u)$ be conjugation gug^{-1} then C_a is equivalent to G_u, and $O(u)$ equivalent to conjugacy class $[a]$. Thus,

$$(G : C_a) = \frac{|G|}{|C_a|} = |[a]|$$

Since p divides G but not C_a, then p divides $(G : C_a)$.

Q3

As shown above, the size of the conjugacy class $[a]$ is $(G : C_a)$

$$k_i = \frac{|G|}{|C_a|}$$

Where $|G|$ has a prime divisor p.

But $k = c + k_s + \cdots + k_t$ where k and all k_i are factors of p, so c is a factor of p.

L. Subgroups of p-Groups (Prelude to Sylow)

A *p-group* is any group whose order is a power of p.

If $|G| = p^k$ then G has a normal subgroup of order p^m for every m between 1 and k.

Q1

Prove there is an element in C such that $\mathrm{ord}(a) = p$

$$|G| = p^k \implies |C| \text{ is a multiple of } p$$

Thus there is an $a \in C$ such that $\mathrm{ord}(a) = p$

Let $x \in C$ st $\langle x \rangle = C$, then $x^{tp} = e$ and then $a = x^t$

Q2

Prove $\langle a \rangle$ is a normal subgroup of G.

Definition of normal subgroup:

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

The center is a normal subgrop.

$\langle a \rangle \subseteq C$, thus $\langle a \rangle$ is a nromal subgroup of G

Q3

Explain why it may be assumed that $G/\langle a \rangle$ has a normal subgroup of order p^{m-1}

$$|G| = p^k \qquad |\langle a \rangle| = p$$

$$\mathrm{ord}(G/\langle a \rangle) = p^{k-1}$$

Thus for m from 1 to k, there is a normal quotient subgroup of order p^{m-1}.

Note:

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \iff \gcd(m, n) = 1$$

Because $\mathrm{ord}((a, b)) = \mathrm{lcm}(m, n) = \frac{mn}{gcd(m,n)} = mn$

Q4

Use J4 to prove that G has a normal subgroup of order p^m.

Correspondence theorem:

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

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

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

Use the natural homomorphism $f : G \to G/\langle a \rangle$ with kernel $\langle a \rangle$

Let S be a the normal subgroup of $G/\langle a \rangle$ whose order is p^{m-1}

Show S^* is a normal subgroup of G and its order is p^m

Since the order of $\langle a \rangle$ is p, and the order of S is p^{m-1} then the order of S^* is p^m

Both S and K are normal subgroups, thus S^* is normal.

M. p-Sylow Subgroups

Q1

Cauchy's theorem states: If G is a group and p is any prime divisor of $|G|$, then G has at least one element of order p.

If q is a prime that divides $|G|$ then there would be an element of order q. Thus the order of any p-group is a power of p.

Q2

Prove every conjugate of a p-Sylow subgroup of G is a p-Sylow subgroup of G.

gHg^{-1} is an inner automorphism hence $|H| = |gHg^{-1}|$

Q3

Let $a \in N$ and suppose the order of Ka in N/K is a power of p. Let $S = \langle Ka \rangle$ be the cyclic subgroup of N/K generated by Ka. Prove that N has a subgroup S^* such that S^*/K is a p-group.

$$N = N(K) = \{g \in G : gK = Kg\}$$

$$f : N \to N/K$$
$$f(a) = Ka$$

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

Hence $xy \in S^*$ and $S^* \leq N$. By J4:

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

$|S|$ is a power of p.

$$|S^*/K| = (S^* : K) = \frac{|S^*|}{|K|} = |S|$$

Q4

Prove that S^* is a p-subgroup of G, then explain why $S^* = K$ and why it follows that $Ka = K$.

$$S = \langle Ka \rangle$$
$$S^* = \{x \in N : Kx \in S\}$$

$$S^* \leq N \text{ and } a \in N$$

$K \leq N$ because normalizer contains the group itself

Let $x \in K$, then $Kx = K \in S$ thus $x \in S^*$, so $K \leq S^*$ but K is maximal, hence $S^* = K$ and it follows $Ka = K$.

Q5

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

Hence $S = \{K\}$

Any $Ka \in N/K$ with order p is equivalent to K the identity.

Q6

$$\text{ord}(a) = p^k \implies a^{p^k} = e$$

$Ka^{p^k} = K$, thus order of Ka in N/K is a power of p.

If $\text{ord}(a)$ is a power of p then $a \in K$

Q7

If $aKa^{-1} = K$ then $a \in N$

$\text{ord}(a)$ is a power of p then $a \in K$

N. Sylow's Theorem

Let G be a finite group and K a p-Sylow subgroup of G.

Let X be the set of all the conjugates of K.

If $C_1, C_2 \in X$, let $C_1 \sim C_2$ iff $C_1 = aC_2a^{-1}$ for some $a \in K$

Q1

Prove $\sim$ is an equivalence relation on X.

$$X = \{aKa^{-1}, \forall a \in G$$

$$C_1, C_2 \in X$$
$$C_1 \sim C_2 \text{ iff } C_1 = aC_2a^{-1} \text{ for an } a \in K$$

Let $u \in X$ st $u \sim C_1$ and $u \sim C_2$

$$\begin{aligned} u = a_1C_1a_1^{-1} &= a_2C_2a_2^{-1} \\ a_1C_1a_1^{-1} &= a_2C_2a_2^{-1} \\ C_1 &= a_1^{-1}a_2C_2a_2^{-1}a_1 \\ &= (a_1^{-1}a_2)C_2(a_1^{-1}a_2)^{-1} \\ &= \bar{a}C_2\bar{a}^{-1} \end{aligned}$$

Thus $C_1 \sim C_2$

Q2

For each $C \in X$, prove the number of elements in $[C]$ is a divisor of $|K|$.

Conclude that for each $C \in X$, the number of elemenbts in $[C]$ is either 1 or a power of p.

From orbit-stablizer:

$$O(C) = \{aCa^{-1} : a \in K\} = [C]$$
$$G_C = \{a \in K : aCa^{-1} = C\} = N(C) = N$$

$$|[C]| = (K : N)$$

Let $\phi : N^* \to [C]$ by $\phi(Na) = aCa^{-1}$

Thus $|O(C)| = |[C]| = \frac{|K|}{|N|}$ and the number of elements in $[C]$ is either 1 or a power of p.

Alternative: from M2, every conjugate of K is also a p-Sylow subgroup of G. Hence from Chapter 14 I10, number of elements in $X_C = [C]$ is a divisor of $|K|$.

Q3

Prove the only class with a single element is $[K]$ (using exercise M7).

$$\begin{aligned} [K] &= \{aKa^{-1} : a \in K\} \\ &= \{K\} \end{aligned}$$

If $|[C]| = 1$ then $C = aCa^{-1} \quad \forall a \in K$ which means $C = K$.

Q4

Prove the number of elements in X is $kp + 1$ usings parts 2 and 3.

$$X = \{K, C_2, C_3, ...\}$$

$$X = \bigcup_i [C_i]$$

Where $[C_i] \cap [C_j] = \emptyset$ or $[C_i] = [C_j]$

But $|[K]| = 1$ while all other C_i is a positive power of p.

Thus $|X| = 1 + kp$

Q5

Prove that $(G : N)$ is not a multiple of p.

$(G : N)$ is the number of equivalency classes that partition G, which divides $kp + 1$ (number of elements in X). It does not divide p, hence $(G : N)$ is a not a multiple of p.

Q6

Prove that $(N : K)$ is not a multiple of p.

$(N : K) = \frac{|N|}{|K|}$ but K is a p-Sylow subgroup so $(N : K)$ is not a multiple of p.

$$(G : K) = (G : N)(N : K)$$

We know $(G : K)$ is not a factor of p, because p is a factor of $|K|$ (from K2), and M5 states no element of N/K has order a power of p.

$\therefore (N : K)$ is not a multiple of p.

Q7

Prove $(G : K)$ is not a multiple of p.

$$(G : K) = (G : N)(N : K)$$

Q8

Let G be a finite group of order $p^k m$ where p is not a factor of m. Conclude every p-Sylow subgroup K of G has order p^k

The only class with a single element is $[K]$ since $aKa^{-1} = K$, all elements where the order is a power of p are in K.

P. Decomposition of a Finite Abelian Group into p-Groups

Let G be an abelian group of order $p^k m$ where p^k and m are relatively prime.

Let G_{p^k} be the subgroup of G consisting of all elements whose order divides p^k.

Let G_m be the subgroup of G consisting of all elements whose order divides m.

Q1

Prove $\forall x \in G$ and integers s and t, $x^{sp^k} \in G_m$ and $x^{tm} \in G_{p^k}$.

p^k and m are coprime. Thus $sp^k + tm = gcd(p^k, m) = 1$

G_{p^k} and G_m are subgroups of order p^k and m respectively because $|G| = p^k m$

$(x^{sp^k})^m = e$ thus $\text{ord}(x^{sp^k})|m$ and $x^{sp^k} \in G_m$

Q2

Let $x \in G$, then because p^k and m are coprime $sp^k + tm = 1$.

Thus $x = x^{sp^k} x^{tm} \in G$

But $x^{sp^k} \in G_m$ and $x^{tm} \in G_{p^k}$. Thus,

$$\begin{aligned} x &= yz \\ &= (x^{tm})(x^{sp^k}) \end{aligned}$$

Q3

By Lagrange's theorem $G_{p^k} \cap G_m \leq G_{p^k}$ and also G_m.

Thus $|G_{p^k} \cap G_m|$ divides $|G_{p^k}|$ and $|G_m| \implies |G_{p^k} \cap G_m|$ divides $\gcd(|G_{p^k}|, |G_m|) = 1$

$$\therefore |G_{p^k} \cap G_m| = 1 = \{e\}$$

Q4

G_{p^k} and G_m are normal subgroups because G is abelian. $G_{p^k} \cap G_m = \{e\}$ and so $G = G_{p^k} G_m$

$$\forall x \in G \qquad \exists y \in G_{p^k} \quad \exists z \in G_m : x = yz$$

Let $\phi : G_{p^k} \times G_m \to G$ by,

$$\phi(y, z) = yz$$

Thus,

$$G \cong G_{p^k} \times G_m$$

Q. Basis Theorem for Finite Abelian Groups

Q1

$$
\begin{aligned}
G' &= \{a_2^{l_2} \cdots a_n^{l_n} : l_i \in \mathbb{Z}, 2 \le i \le n\} \\
&= [a_2, \dots, a_n]
\end{aligned}
$$

$\forall x, y \in G'$ then $xy \in G'$

Also by D2, $a_1^{l_1} = a_2^{l_2} = \cdots = a_n^{l_n} = e$, thus contains the identity.

G' contains inverses. Thus $G' \le G$

Q2

Prove:

$$G \cong \langle a_1 \rangle \times G'$$

$$a_1^{k_1} \in \langle a_1 \rangle$$

See also this question

From Chapter 14, H: if H and K are normal subgroups of G, such that $H \cap K = \{e\}$ and $G = HK$, then $G \cong H \times K$

Firstly all subgroups of G are normal since the group is abelian.

Lastly we have to prove that $\langle a \rangle \cap G' = \{e\}$

By Lagrange's theorem $\langle a \rangle \cap G' \le \langle a \rangle$ and also G'.

Thus $|\langle a \rangle \cap G'|$ divides $|\langle a \rangle|$ and $|G'| \implies |\langle a \rangle \cap G'|$ divides $\gcd(|\langle a \rangle|, |G'|) = 1$

$$\therefore |\langle a \rangle \cap G'| = 1 = \{e\}$$

Q3

Explain why we may assume that $G/H = [Hb_1, \dots, Hb_n]$ for some $b_1, \dots, b_n \in G$

Page 149 Theorem 4 from Quotient Groups: "G/H is a homomorphic image of G"

$$f : G \to G/H$$

$$f(x) = Hx$$

Let $x \in G$, then $x = a^{k_0} b_1^{k_1} \cdots b_n^{k_n}$ for some $a, b_1, \dots, b_n \in G$

$$
\begin{aligned}
f(x) &= f(ab_1^{k_1} \cdots b_n^{k_n}) \\
&= H(a \cdot b_1^{k_1} \cdots b_n^{k_n}) = H(b_1^{k_1} \cdots b_n^{k_n}) \qquad \text{(because } a \in H) \\
&= (Hb_1)^{k_1} \cdots (Hb_n)^{k_n}
\end{aligned}
$$

Now,

$$
\begin{aligned}
G/H &= \{f(x) : \forall x \in G\} \\
&= \{(Hb_1)^{k_1} \cdots (Hb_n)^{k_n} : k_i \in \mathbb{Z}, 1 \le i \le n\} \\
&= [Hb_1, \dots, Hb_n]
\end{aligned}
$$

Q4

$x \in G \implies x \in Hx$

But $H = \langle a \rangle$ and $G = [Hb_1, \dots, Hb_n]$.

Thus $x = a^{k_0} b_1^{k_1} \cdots b_n^{k_n}$

Q5

Prove that if $a^{l_0} b_1^{l_1} \cdots b_n^{l_n} = e$, then $a^{l_0} = b_1^{l_1} = \cdots = b_n^{l_n} = e$. Conclude that $G = [a, b_1, \dots, b_n]$.

$$x = a^{l_0} b_1^{l_1} \cdots b_n^{l_n} = e$$
$$G \cong G_1 \times G_2 \times \cdots \times G_n$$
$$G/H \cong G_1/H \times G_2/H \times \cdots \times G_n/H$$

$$\begin{aligned} Hx &= (Ha^{l_0})(Hb_1^{l_1}) \cdots (Hb_n^{l_n}) \\ &= (Hb_1^{l_1}) \cdots (Hb_n^{n}) \end{aligned}$$

Chapter 10, E4: "If m and n are relatively prime, then $\operatorname{ord}(ab) = mn$"

Also $\gcd(a, b) = 1 \implies \gcd(a^i, b^j) = 1$

$$\operatorname{ord}(Hx) = \operatorname{ord}(Hb_1^{l_1}) \cdots \operatorname{ord}(Hb_n^{l_n})$$

Since $\operatorname{ord}(Hx) = 1$, this means $\operatorname{ord}(Hb_i^{l_i}) = 1$ and because $\operatorname{ord}(b_i) = \operatorname{ord}(Hb_i)$, thus $\operatorname{ord}(b_i^{l_i}) = 1 \implies b_i = e$.

Lastly $a^{l_0} \cdot e = e \implies a = e$

Q6

If $|G|$ has the following factorization into primes: $|G| = p_1^{k_1} \cdots p_n^{k_n}$, then $G \cong G_1 \times \cdots \times G_n \cong \langle a_1 \rangle \times \cdots \times \langle a_n \rangle$.

As shown in previous exercise, the order of G is the product of the order of each generator for the subgroups.

Lastly chapter 10, E3 showed that is m and n are relatively prime, then the products $a^i b^j (0 \le i \le m, 0 \le j \le n)$ are all distinct. Thus the products of a and b can be decomposed as unique factors.