Abstract Algebra by Pinter, Chapter 15

Amir Taaki

Chapter 15 on Quotients

Contents

Section A

Q1

Let $G = \mathbb{Z}_1 0, H = \{0, 5\}$. Explain why $G/H \cong \mathbb{Z}_5$

Elements of G/H:

$$\begin{aligned} H + 0 &= \{0, 5\} \\ H + 1 &= \{1, 6\} \\ H + 2 &= \{2, 7\} \\ H + 3 &= \{3, 8\} \\ H + 4 &= \{4, 9\} \end{aligned}$$

$G/H \cong \mathbb{Z}_5$ because let the isomorphism $f(Hx) = x$ then $f(Hx \cdot Hy) = f(Hx)f(Hy)$.

Q2

Let $G = S_3$ and $H = \{\epsilon, \beta, \delta\}$

$\epsilon = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right)$ $\alpha = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$ $\beta = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right)$

$\gamma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right)$ $\delta = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$ $\kappa = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right)$

Elements of the quotient group:

$$\begin{aligned} H = H\epsilon &= \{\epsilon, \beta, \delta\} \\ H\alpha &= \{\alpha, \kappa, \gamma\} \end{aligned}$$

Q3

Let $G = D_4$ and $H = \{R_0, R_2\}$

Elements of G/H:

$$
\begin{aligned}
H &= \{R_0, R_2\} \\
HR_1 &= \{R_1, R_3\} \\
HR_4 &= \{R_4, R_5\} \\
HR_6 &= \{R_6, R_7\}
\end{aligned}
$$

Symbol	Transform
R_0	Identity
R_1	Rotate 90
R_2	Rotate 180
R_3	Rotate 270
R_4	Flip left diagonal
R_5	Flip right diagonal
R_6	Flip horizontal
R_7	Flip vertical

Q4

Let $G = D_4$ and $H = \{R_0, R_2, R_4, R_5\}$. Elements are H, HR_1.

Q5

Let $G = \mathbb{Z}_4 \times \mathbb{Z}_2, H =< (0, 1) >$.

$$
\begin{aligned}
H &= \{(0, 0), (0, 1)\} \\
H + (1, 0) &= \{(1, 0), (1, 1)\} \\
H + (2, 0) &= \{(2, 0), (2, 1)\} \\
H + (3, 0) &= \{(3, 0), (3, 1)\}
\end{aligned}
$$

Q6

Let $G = P_3, H = \{\emptyset, \{1\}\}$.

$$
\begin{aligned}
H &= \{\emptyset, \{1\}\} \\
H \cap \{2\} &= \{\{2\}, \{1, 2\}\} \\
H \cap \{3\} &= \{\{3\}, \{1, 3\}\} \\
H \cap \{2, 3\} &= \{\{2, 3\}, \{1, 2, 3\}\}
\end{aligned}
$$

Section B

Q1

$H = \{(x, 0) : x \in \mathbb{R}\}$

a

For any $a \in H$ and $x \in G = \mathbb{R} \times \mathbb{R}$ then $xax^-1 \in H$ therefore $H \trianglelefteq G$.

b

Elements of $G/H = \{H + (0, y) : y \in \mathbb{R}\}$.

c

Coset addition

Q2

$H = \{(x, y) : y = -x\}$

a

For any $a \in H$ and $x \in G = \mathbb{R} \times \mathbb{R}$ then $xax^{-1} \in H$ therefore $H \trianglelefteq G$.

b

Elements of $G/H = \{H + (0, y) : y \in \mathbb{R}\}$.

c

Coset addition

Q3

$H = \{(x, y) : y = 2x\}$

a

Let $(\bar{x}, \bar{y}) \in H$ and $(u, v) \in \mathbb{R} \times \mathbb{R}$.

Then $(u, v)(\bar{x}, \bar{y})(u, v)^{-1} = (\bar{x}, \bar{y}) \in \mathbb{R} \times \mathbb{R}$, therefore $H \trianglelefteq G$.

b

Elements of $G/H = \{H + (0, y) : y \in \mathbb{R}\}$.

c

Coset addition

Section C

Q1

If $x^2 \in H$ for every $x \in G$ then every element of G/H is its own inverse.

Let there be a coset Hx, then $x^2 \in H$. So $\therefore x^2 H = Hx^2 = H$. So H is the identity coset.

$(Hx)(Hx) = Hx^2 = H$.

So every element of G/H is its own inverse.

Likewise if every element of G/H is its own inverse, then $(Hx)(Hx) = H \implies x^2 \in H$.

Q2

Let m be a fixed integer. If $x^m \in H$ for every $x \in G$ then the order of every element in G/H is a divisor of m.

Let there be an element $y \in G$ st. $y^m \in H$ where $m = qn$, therefore $(y^n)^q \in H$ where $ord(y) = n$. Then:

$$(Hy)^n = (Hy) \cdots (Hy) = Hy^n = H$$

Conversely if the order of every element in G/H is a divisor of m, then $x^m \in H$ for every $x \in G$.

This holds true because $ord(x) = n$, then $x^n = e = (x^n)^q = x^m$, where $m = qn$.

$$\therefore x^m \in H$$

Let $h = Hx$ then $ord(h) = n$ because $(Hx)^n = Hx^n = H$ because $x^n \in H$.

Q3

Suppose that for every $x \in G$, there is an integer n st. $x^n \in H$.

Then every element of G/H has a finite order. By previous exercise this is shown.

Q4

Every element of G/H has a square root iff for every $x \in G$, there is some $y \in G$ st. $xy^2 \in H$.

$$xy^2 \in \implies xy^2 = h \text{ where } h \in H$$

$\therefore x = hy^{-2}$ but since $y \in G$ and G is closed, there exists $\bar{y} \in G$ st. $\bar{y} = y^{-1}$ and $\therefore x = h\bar{y}^2$ and $x \in H\bar{y}^2$.

Theorem 5 also states:

iff $xy^2 \in H$ then $Hx = Hy^{-2} = (Hy)^{-2}$.

Q5

G/H is cyclic iff there is an element $a \in G$ that $\forall x \in G$, $\exists$ integer n st. $xa^n \in H$.

$$\begin{aligned} xa^n \in H \implies Hx &= Ha^{-n} \\ &= (Ha)^{-n} = (Ha^{-1})^n \end{aligned}$$

Thus G/H is cyclic since $(Ha^{-1})^n \in G/H$ because $a^{-1} \in G$.

Q6

G is abelian, H_p is the set of all $x \in G$ whose order is a power of p. Prove H_p is a subgroup of G.

Property 1: closure

Let $x, y \in H_p$, then $ord(x) = p^k$ and $ord(y) = p^l$. That is, $x^{p^k} = e = y^{p^l}$.

Let $(xy)^{p^m} = e = x^{p^m} y^{p^m} \therefore m = lcm$ and $xy \in H_p$

Property 2: inverses

Let $x \in H_p$ and $e \in H_p$

$$\begin{aligned} x \cdot x^{-1} = e &= (x \cdot x^{-1})^{p^k} \\ &= x^{p^k}(x^{-1})^{p^k} = (x^{-1})^{p^k} = e \\ \therefore x^{-1} \in H_p & \end{aligned}$$

Second part: prove that G/H_p has no elements who order is a nonzero power of p.

Let $x \in G$ st $Hx \neq H_p$ and $ord(Hx) = p^k$.

Then $(Hx)^{p^k} = H_p$

$$\begin{aligned} \therefore h_1^{p^k} x^{p^k} &= h_2 \\ x^{p^k} &= h_2 h_1^{-p^k} \end{aligned}$$

But $h_2 \in H_p$ and $h_1 \in H_p$

$$\therefore x^{p^k} = h \text{ where } h \in H_p$$

$$\therefore x^{p^k} \in H_p$$

But $x^{p^k} \in Hx \neq H_p$. Proof by contradiction.

Q7

a

If G/H is abelian then:

$$HxHy = HyHx \text{ or } Hxy = Hyx$$

So $h_1xy = h_2yx$ where $h_1, h_2 \in H$

$$\begin{aligned} xy &= h_1^{-1}h_2yx \\ xyx^{-1} &= h_1^{-1}h_2y \\ xyx^{-1}y^{-1} &= h_1h_2 \in H \end{aligned}$$

So all commutators of G are in H iff G/H is abelian.

b

$H \trianglelefteq K \trianglelefteq G$ and G/H is abelian. Prove G/K and K/H are both abelian.

From page 152, if G/H is abelian, then it contains all the commutators of G.

Since $H \trianglelefteq K$, then:

$$Hxy = Hyx \text{ or } xy(xy)^{-1} \in H$$

Since all commutators are in H and $H \trianglelefteq K$, then G/H is abelian and so also G/K because all commutators are also in K.

$$\begin{gathered} K/H \text{ is abelian} \implies Hx, Hy \in K/H \\ xyx^{-1}y^{-1} \in H \\ Hxyx^{-1}y^{-1} = H \\ Hxy = Hyx \end{gathered}$$

So K/H is abelian.

Section D

Q1

If every element of G/H has finite order, and every element of H has finite order, then every element of G has finite order.

For every $h \in G/H$, $ord(h)$ is a divisor of $(G : H)$ by lagrange's theorem.

$$(G : H) = \frac{ord(G)}{ord(H)}$$

$$ord(G) = (G : H)ord(H)$$

But $ord(h)$ is a divisor of $(G : H)$. So:

$$ord(G) = (k \cdot ord(h))ord(H)$$

Q2

If every element of G/H has a square root, and every element of H has a square root, then every element of G has a square root. (Assume G is abelian.)

Let $Hx \in G/H$ and $h \in H$.

If $x = y^2$ for some $y \in G$ and $h = \bar{h}^2$ for some $\bar{h} \in H$, then $hx = \bar{h}^2 y^2 = (\bar{h}y)^2$ since G is abelian.

Q3

G/H and H are p-groups $\implies \forall Hx \in G/H, (Hx)^{p^k} = H$

Because $H \trianglelefteq G$, $(Hx)^{p^k} = (Hx) \cdots (Hx) = Hx^{p^k}$, then:

$$x^{p^k} = h \in H$$

But,

$$\begin{aligned}
h^{p^l} &= e \\
(x^{p^k})^{lcm(l,k)} &= e^{lcm(l,k)} = e \\
\therefore x^{p^{k \cdot lcm(l,k)}} &= e
\end{aligned}$$

So every element of G is a power of prime p.

Q4

Let H be generated by $\{h_1, \cdots, h_n\}$ and let G/H be generated by $\{Ha_1, \cdots, Ha_m\}$. Thus every element x in G can be written as a linear combination of h_i and a_j.

Section E

Q1

For each element $a \in G$, the order of the element Ha in G/H is a divisor of the order of a in G.

From Chapter 14, F1, if $f : G \to H$, then for each element $a \in G$, let $ord(a) = n$, then $a^n = e$ and $f(a^n) = (f(a))^n$, therefore the order of $f(a)$ is a divisor of the order of a because $f(a^n) = f(e) = e_H$.

So therefore for each each element $a \in G$, let $ord(a) = n$, then $a^n = e$.

Then $(Ha)^n = He$ and so the order of Ha in G/H is a divisor of the order of a in G.

Q2

If $(G : H) = m$, the order of every element of G/H is a divisor of m.

$(G : H)$ is the order of G/H.

By theorem 5 (page 129): "the order of any element of a finite group divides the order of the group."

So if $(G : H) = m$, the order of every element of G/H is a divisor of m.

Q3

If $(G : H) = p$ where p is a prime, then the order of every element $a \notin H$ in G is a multiple of p.

From theorem 5:

$$(G : H) = \frac{ord(G)}{ord(H)}$$

That is:

$$\begin{aligned} ord(G) &= (G:H)ord(H) \\ &= p \cdot ord(H) \end{aligned}$$

Since the order of every element of G is a divisor of the order of G, then:

$$ord(a) = q \text{ and } ord(G) = qn$$
$$= p \cdot ord(H)$$

It follows that since $q|pord(H)$ and $q \perp p$, then $q|ord(H)$ and so is a multiple of p.

Q4

If G has a normal subgroup of index p, where p is a prime, then G has at least one element of order p.

$H \trianglelefteq G$ st $(G:H) = p$ where p is prime.

$$ord(G/H) = p$$

The order of G/H is prime, thus it is cyclic.

Cauchy's theorem (page 131): "if G is a finite group, and p is a prime divisor of $|G|$, then G has an element of order p."

Theorem 4 (page 129): "If G is a group with a prime number p of elements, then G is a cyclic group. Furthermore, any element $a \neq e$ in G is a generator of G."

So then $(G/H) \cong \mathbb{Z}_p$

Q5

If $(G:H) = m$, then $a^m \in H$ for every $a \in G$.

By Q2, $ord(Hx)$ is a divisor of m.

So $(Ha)^m = H$ but $H^m = H$ and H is a normal subgroup of G, so $a^m \in H$.

Q6

In $\mathbb{Q}/\mathbb{Z}$, every element has finite order.

$$\mathbb{Q} = \{p_1/q_1 : p_1q_1 = p_2q_2 \forall p_1, p_2, q_1, q_2 \in \mathbb{Z}\}$$

Where (p_1, q_1) (p_2, q_2) iff $p_1q_1 = p_2q_2$.

$$\mathbb{Q}/\mathbb{Z} = \{m/n + \mathbb{Z} : m, n \in \mathbb{Z}\}$$

Let $h \in \mathbb{Z}$, then $h^x \in \mathbb{Z}$ for any $x \in \mathbb{Z}$.

Then for any $g \in \mathbb{Q}/\mathbb{Z}$, g^x is a coset of $m/n + \mathbb{Z}$

Therefore every element in $\mathbb{Q}/\mathbb{Z}$ has finite order.

Section F

Q1

For every $x \in G$, there is some integer m such that $Cx = Ca^m$.

$$G/C =< Ca >= \{(Ca)^m : m \in \mathbb{Z}\}$$

Now for $x \in G, Cx \in G/C$

$$\therefore \exists m : Cx = Ca^m$$

Q2

For every $x \in G$, there is some integer m such that $x = ca^m$, where $c \in C$.

$$Cx = Ca^m \implies c_1 x = c_2 a^m \text{ where } c_1, c_2 \in C$$

$$\begin{aligned} c_1 x &= c_2 a^m \\ &= c_1^{-1} c_2 a^m \end{aligned}$$

But C is closed so $c_1^{-1} c_2 = c \in C$. So:

$$x = ca^m$$

Q3

For any two elements x and y in G, $xy = yx$.

$$\begin{aligned} x &= c_1 a^m \\ y &= c_2 a^n \\ xy &= c_1 a^m c_2 a^n \end{aligned}$$

But for any $c \in C$ and $x \in G$,

$$xc = cx$$

And $c_1, c_2 \in G$, so $c_1 c_2 = c_2 c_1$.

$$\begin{aligned} xy &= c_1 a^m c_2 a^n \\ a^{-n} xy &= c_1 a^m c_2 \\ c_2^{-1} a^{-n} xy &= c_1 a^m \\ (a^n c_2)^{-1} xy &= c_1 a^m \\ (a^n c_2)^{-1} x &= c_1 a^m y^{-1} \end{aligned}$$

But,

$$\begin{aligned} a^n c_2 &= c_2 a^n \\ y^{-1} x &= c_1 a^m y^{-1} \\ y^{-1} x &= xy^{-1} \\ xy &= yx \end{aligned}$$

Q4

If G/C is cyclic then:

$$x = ca^m \text{ for every } x \in G$$

And for any two elements in G, $xy = yx$.

Therefore G is abelian.

Section G

Using the class equation to determine the size of the center.

Q1

Conjugancy class of a is:

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

The center of G is:

$$C = \{a \in G : xa = ax, \forall x \in G\}$$

If $a \in C$ then for all $x \in G$:

$$\begin{aligned} xa &= ax \\ xax^{-1} &= a \end{aligned}$$

This means the conjugancy class of a contains a (and no other element).

Q2

Let c be the order of C. Then $|G| = c + k_s + k_s + k_{s+1} + \cdots + k_t$, where $k_s, \cdots, k_t$ are the sizes of all the distinct conjugacy classes of elements $x \notin C$.

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

If $a \in C$ then $xax^{-1} = a$ for all \$$x \in G$ and $[a] = \{a\}$.

So $c = k_1 + \cdots + k_{s-1}$ and $|G| = c + k_s + \cdots + k_t$ where $k_s, \cdots, k_t$ are sizes of distinct conjugacy classes of elements $a \notin C$.

Q3

For each $i \in \{s, s+1, \cdots, t\}$, k_t is equal to a power of p.

Chapter 13, I6 states "the size of every conjugancy class is a factor of |G|". $|G| = p^k$ so $|S_i| = k_i$ must equal some factor of p^k, that is, there is some p^m which divides p^k.

Q4

See this video at 17:20 for the proof.

Explain why c is a multiple of p.

From orbit-stabilizer $k_i = \frac{|G|}{|C_x|}$ 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 also.

Q5

If $|G| = p^2$, G must be abelian.

By lagrange's theorem $|C|||G|$.

Possibilities are $\{1, p, p^2\}$.

$|C| \neq 1$ because center is non-trivial.

If $|C| = p$, then G/C has p cosets, therefore G/C is cyclic and hence abelian (from part F).

Else $|C| = p^2$ means C is entire group and abelian.

Q6

Any group of size p^2 is isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

To see why, if there is an element $< a >= \mathbb{Z}_{p^2}$ then the group is isomorphic to $\mathbb{Z}_{p^2}$.

If not then by lagrange's theorem, the subgroup must have order p, in which case the group is isomorphic $\mathbb{Z}_p \times \mathbb{Z}_p$ by the mapping:

$$f(x) : G \to \mathbb{Z}_p \times \mathbb{Z}_p$$

By $f(ab) = (a, b)$.

See also Cayley's theorem on page 96.

Section H

Q1

If $ord(a) = tp$ where $a \in G$, what element of G has order p?

$$ord(a) = tp \implies a^{tp} = e = (a^t)^p$$

Therefore $ord(a^t) = p$

Q2

Now $ord(a)$ is not a multiple of p. Then $G/ < a >$ is a group with fewer than k elements and its order is a multiple of p.

$|G| = k = np$ where p is prime but $ord(a)$ is not a multiple of p.

By lagrange's theorem $ord(a)$ must divide $|G|$ since $< a >$ is a subgroup of G.

$ord(a)|k$ or $ord(a)|np$, but since $ord(a) \perp p$ then $ord(a)|n$.

The order of $G/ < a >$ is the same as the number of cosets of $< a >$.

$$\begin{aligned} ord(G/ < a >) &= (G :< a >) \\ &= \frac{ord(G)}{ord(a)} \end{aligned}$$

Since $ord(a)$ is not a multiple of p, but $|G|$ is, then $ord(G/ < a >)$ is a multiple of p.

Q3

Since $ord(G/ < a >)$ is a multiple of p, by Cauchy's theorem, p is a prime divisor of the group, then $G/ < a >$ has an element of order p.

Q4

By E1, G has an elemtn of order p, by an isomorphism from $f(a) = \bar{a}$.