Homework 7

Aleck Zhao

November 3, 2016

Section 2.10: The Isomorphism Theorem

22. Show that $\mathbb{R}^*/\{1,-1\} \cong \mathbb{R}^+$.

Solution. Define the mapping $\varphi : \mathbb{R}^* \to \mathbb{R}^+$ given by $\varphi(x) = x^2$ for $x \in \mathbb{R}^*$. This is indeed a homomorphism:

$$\varphi(xy) = (xy)^2 = x^2y^2 = \varphi(x)\varphi(y)$$

and the kernel is the set $\{1,-1\}$ since $\varphi(1) = \varphi(-1) = 1$. Here, the image of $\mathbb{R}^*$ under φ is exactly $\mathbb{R}^+$, since the square of non-zero elements of $\mathbb{R}$ are positive. Thus, by the Isomorphism theorem,

$$\varphi``(\mathbb{R}^*) = \mathbb{R}^+ \cong \mathbb{R}^*/\ker\varphi = \mathbb{R}^*/\{1,-1\}$$

as desired.

$\square$

29. Let $G = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \middle| a,b,c \in \mathbb{R} \right\}$.

(a) Show that G is a subgroup of $M_3(\mathbb{R})^*$ and that $Z(G) \cong \mathbb{R}$.

Proof. Clearly $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in G$ which is the identity in $\mathrm{GL}_3(\mathbb{R})$. Then let

$$A = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$
$$M = \begin{bmatrix} 1 & m & n \\ 0 & 1 & p \\ 0 & 0 & 1 \end{bmatrix}$$

be in G, so their product

$$AM = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & m & n \\ 0 & 1 & p \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & m+a & n+ap+b \\ 0 & 1 & p+c \\ 0 & 0 & 1 \end{bmatrix}$$

is also in G. Finally, the inverse of A is given by

$$A^{-1} = \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix}$$

which is also in G. Thus, G is a subgroup of $\mathrm{GL}_3(\mathbb{R}_)$, as desired.
Let $M \in Z(G)$. Then we have

$$AM = \begin{bmatrix} 1 & m+a & n+ap+b \\ 0 & 1 & p+c \\ 0 & 0 & 1 \end{bmatrix}$$
$$MA = \begin{bmatrix} 1 & a+m & b+mc+n \\ 0 & 1 & c+p \\ 0 & 0 & 1 \end{bmatrix}$$

so since $M \in Z(G)$, we must have $AM = MA$, which is equivalent to having $n+ap+b = b+mc+n$ or $ap = mc$. Since a and c can be anything, it must be the case that $m = p = 0$. Thus, the general form of $M \in Z(G)$ is

$$M = \begin{bmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad n \in \mathbb{R}$$

and we can construct a mapping $\varphi : Z(G) \to \mathbb{R}$ where

$$\varphi\left(\begin{bmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) = n$$

which is obviously bijective. It is also a homomorphism because

$$\varphi\left(\begin{bmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & m \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}\right) = \varphi\left(\begin{bmatrix} 1 & 0 & m+n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) = m+n$$
$$\varphi\left(\begin{bmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) + \varphi\left(\begin{bmatrix} 1 & 0 & m \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) = m+n$$

Thus $Z(G) \cong \mathbb{R}$, as desired.

□

(b) Show that $G/Z(G) \cong \mathbb{R} \times \mathbb{R}$.

Proof. Construct a mapping $\varphi : G \to \mathbb{R} \times \mathbb{R}$ where

$$\varphi\left(\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}\right) = (a, c)$$

If we take A and M as above, then

$$AM = \begin{bmatrix} 1 & m+a & n+ap+b \\ 0 & 1 & p+c \\ 0 & 0 & 1 \end{bmatrix}$$

so $\varphi(AM) = (m+a, p+c)$ while

$$\varphi(A) + \varphi(M) = (a, c) + (m, p) = (a+m, c+p)$$

so φ is a homomorphism where $\varphi``(G) = \mathbb{R} \times \mathbb{R}$ since $a, c \in \mathbb{R}$. Here, $\ker \varphi$ is exactly the set of matrices where $b \in \mathbb{R}$ and $(a, c) = (0, 0)$, so $a = c = 0$, which is exactly $Z(G)$. Thus, by the Isomorphism theorem,

$$\varphi``(G) = \mathbb{R} \times \mathbb{R} \cong G/\ker\varphi = G/Z(G)$$

as desired.

□

Section 8.2: Cauchy's Theorem

7. If H and K are conjugate subgroups in G, show that $N(H)$ and $N(K)$ are conjugate.

Proof. Let $H = g_0 K g_0^{-1}$ for some $g_0 \in G$. Then we have

$$\begin{aligned} N(H) &= \{ g \in G \mid gHg^{-1} = H \} \\ &= \{ g \in G \mid g(g_0 K g_0^{-1})g^{-1} = g_0 K g_0^{-1} \} \\ &= \{ g \in G \mid (g_0^{-1} g g_0) K (g_0^{-1} g^{-1} g_0) = K \} \\ &= \{ g \in G \mid (g_0^{-1} g g_0) K (g_0^{-1} g g_0)^{-1} = K \} \end{aligned}$$

so the set given by $g_0^{-1} N(H) g_0$ is exactly

$$g_0^{-1} N(H) g_0 = \{ g_0^{-1} g g_0 \in G \mid (g_0^{-1} g g_0) K (g_0^{-1} g g_0) = K \} = \{ g_1 \in G \mid g_1 K g_1^{-1} = K \} = N(K)$$

so $N(H) = g_0 N(K) g_0^{-1}$, thus $N(H)$ and $N(K)$ are conjugate, as desired.

□

14. Let $D_3 = \{1, a, a^2, b, ba, ba^2\}$ where $o(a) = 3, o(b) = 2, aba = b$. If $H = \{1, b\}$, show that $N(H) = H$.

Proof. Since $N(H)$ is a subgroup of D_3 so its order must divide 6. Since H is a subgroup of D_3, it is also a subgroup of $N(H)$, so $|H| = 2 \mid |N(H)|$. Thus, $|N(H)|$ is even and divides 6, so $|N(H)| = 2$ or 6. $N(H)$ can't possibly be all of D_3 since $ab \neq ba$, so we must have $|N(H)| = 2$, so in fact $N(H) = H$ since $N(H)$ contains H.

□

23. Let G^ω be the group of sequences $[g_i) = (g_0, g_1, \cdots)$ from a group G with component-wise multiplication $[g_i) \cdot [h_i) = [g_i h_i)$. Show that if $G \neq \{1\}$ is a finite p-group, then G^ω is an infinite p-group.

Proof. Since G is a finite p-group, suppose $|G| = p^n$ for some $n \geq 1$. Thus, $g^{p^n} = 1$ for any $g \in G$. Thus, for any sequence $[g_i) = (g_0, g_1, \cdots)$, we have

$$\begin{aligned} [g_i)^{p^n} &= (g_0^{p^n}, g_1^{p^n}, \cdots) \\ &= (1, 1, \cdots) \end{aligned}$$

thus $o([g_i))$ must divide p^n for any $[g_i) \in G^\omega$, so G^ω is a p-group. Clearly G^ω is not a finite group, in fact it is not even countable.

□

26. Let G be a non-abelian group of order p^3 where p is a prime. Show that

(a) $Z(G) = G'$ and this is the unique normal subgroup of G of order p.

Proof. Since $Z(G)$ is a subgroup of G, we must have $|Z(G)| \mid p^3$. By Theorem 6, since G is a finite p-group, its center is not $\{1\}$. Thus, we must have one of the following:

$$|Z(G)| = p, p^2, p^3$$

We can't have $|Z(G)| = p^3$ because then $Z(G) = G$ but we assumed G was non-abelian. If $|Z(G)| = p^2$, then $G/Z(G)$ is a well-defined group since $Z(G) \trianglelefteq G$. However, this means the $G/Z(G)$ has order $p^3/p^2 = p$, so $G/Z(G)$ must be an abelian cyclic group. This implies G was abelian to begin with, which is a contradiction.
Thus, we must have $|Z(G)| = p$. Since $Z(G)$ is normal in G, it is the only subgroup of order p, as desired.

□

(b) G has exactly $p^2 + p - 1$ distinct conjugacy classes.

Proof. By the class equation, we have

$$|G| = |Z(G)| + \sum |G : N(a_i)|$$

where a_i are the representatives of the conjugacy classes. We must have $|G : N(a_i)|$ divides the order of G, so $|G : N(a_i)| = p, p^2, p^3$ since we assume a_i is not in the center. We can't have it be p^3, since the center is non-empty. If $|G : N(a_i)| = p^2$ for some a_i, then

$$\frac{|G|}{|N(a_i)|} = \frac{p^3}{|N(a_i)|} = p^2 \implies |N(a_i)| = p$$

Thus, since $Z(G)$ is the unique subgroup of order p, we must have $N(a_i) = Z(G)$. Thus, $a_i \in Z(G)$, but we assumed otherwise, contradiction.

Thus, we must have $|G : N(a_i)| = p$ for all a_i representatives not in the center. By the class equation, we have

$$p^3 = p + \sum p \implies p^3 - p = p(p^2 - 1) = \sum p$$

so there are $p^2 - 1$ distinct conjugacy classes that are not in the center, and $|Z(G)| = p$, so there are p singleton conjugacy classes. Thus, the total number of conjugacy classes is $p^2 + p - 1$, as desired.

□

Section 8.3: Group Actions

3. If p and q are primes, show that no group of order pq is simple.

Proof. By Cauchy's theorem, p divides pq so there exists an element of order p. Suppose $o(g) = p$ for some $g \in G$. Then $|\langle g\rangle| = g$, so $|G : \langle g\rangle| = q$. WLOG $q \leq p$, so by Corollary 1 of Theorem 1, $\langle g\rangle \trianglelefteq G$, so G is not simple.

□

13. Let $G = (\mathbb{R}, +)$ and define $a \cdot z = e^{ia}z$ for all $z \in \mathbb{C}$ and $a \in G$. Show that $\mathbb{C}$ is a G-set, describe the action geometrically, and find all orbits and stabilizers.

Proof. We have $0 \in \mathbb{R}$ is the identity, so $0 \cdot z = e^{i\cdot 0}z = z$. If $a, b \in \mathbb{R}$, we have

$$a \cdot (b \cdot z) = a \cdot (e^{ib}z) = e^{ia}(ze^{ib}) = e^{i(a+b)}z$$
$$(ab) \cdot z = (a + b) \cdot z = e^{i(a+b)}z$$

Thus, G acts on $\mathbb{C}$ so $\mathbb{C}$ is a G-set, as desired.

This action is equivalent to a rotation by an angle $a \in \mathbb{R}$ where a is in radians. The orbits are the concentric circles about the origin with $r \geq 0$, each circle being an orbit. The stabilizers are of the form $2k\pi \in \mathbb{R}$ where $k \in \mathbb{Z}$, since a rotation by a multiple of 2π does not change the position.

□

21. If H is a subgroup of G, find a G-set X and an element $x \in X$ such that $H = S(x)$.

Solution. Let $X = G$, and define the group action as follows for all $x \in G$:

$$g \cdot x = \begin{cases} x & \text{if } g \in H \\ 1 & \text{if } g \notin H \end{cases}$$

We may check that this is indeed a group action. We have $1 \cdot x = x$ since $1 \in H$ because H is a subgroup. Next, consider two elements $g, h \in G$. There are 4 cases:

$$\begin{aligned} g, h \in H \implies gh \in H \quad (1) \\ \implies g \cdot (h \cdot x) = g \cdot x = x = (gh) \cdot x \\ g \in H, h \notin H \implies gh \notin H \quad (2) \\ \implies g \cdot (h \cdot x) = g \cdot 1 = 1 = (gh) \cdot x \\ g \notin H, h \in H \implies gh \notin H \quad (3) \\ \implies g \cdot (h \cdot x) = g \cdot x = 1 = (gh) \cdot x \\ g, h \notin H \implies gh \notin H \quad (4) \\ \implies g \cdot (h \cdot x) = g \cdot 1 = 1 = (gh) \cdot x \end{aligned}$$

thus, $X = G$ is indeed a G-set under this action. Then, for any $h \in G$ such that $h \neq 1$, the stabilizer $S(h)$ all elements $g \in G$ such that $g \cdot h = h$. The g that fit this are the $g \in H$, so $H = S(h)$, as desired.

□

23. Let X be a G-set and let x and y denote elements of X.

(a) Show that $S(x)$ is a subgroup of G.

Proof. Clearly $1_g \cdot x = x$ because X is a G-set. Next, if $g, h \in S(x)$, we have

$$\begin{aligned} g \cdot x = x = h \cdot x \\ \implies g \cdot (h \cdot x) = x \\ \implies (gh) \cdot x = x \end{aligned}$$

so $gh \in S(x)$ as well. Finally, if $g \in S(x)$, we have

$$\begin{aligned} g \cdot x = x \\ \implies g^{-1}(g \cdot x) = g^{-1} \cdot x \\ \implies x = g^{-1} \cdot x \end{aligned}$$

so $g^{-1} \in S(x)$ as well. Thus, $S(x)$ is a subgroup of G, as desired

□

(b) If $x \in X$ and $b \in G$, show that $S(b \cdot x) = bS(x)b^{-1}$.

Proof. We have

$$\begin{aligned} S(b \cdot x) &= \{ g \in G \mid g \cdot (b \cdot x) = b \cdot x \} \\ &= \{ g \in G \mid (gb) \cdot x = b \cdot x \} \\ &= \{ g \in G \mid (b^{-1}gb) \cdot x = x \} \\ b^{-1}S(b \cdot x)b &= \{ b^{-1}gb \in G \mid (b^{-1}gb) \cdot x = x \} \\ &= \{ h \in G \mid h \cdot x = x \} \\ &= S(x) \end{aligned}$$

so $S(b \cdot x) = bS(x)b^{-1}$ as desired.

□

(c) If $S(x)$ and $S(y)$ are conjugate subgroups, show that $|G \cdot x| = |G \cdot y|$.

Proof. Let $S(x) = aS(y)a^{-1}$ for some $a \in G$. Then define the mapping

$$\varphi : G \cdot x \to G \cdot y$$

by $\varphi(g \cdot x) = (ag) \cdot x$. This is well defined: if $g_1 \cdot x = g_2 \cdot x$, then $g_2 g_1^{-1} \in S(x)$, so the conjugate

$$a(g_2 g_1^{-1})a^{-1} = (ag_2)(ag_1)^{-1} \in S(y)$$

so

$$(ag_2) \cdot x = (ag_1) \cdot x$$

This also means that φ is 1-1 because we can simply recover the g_1 and g_2. Clearly φ is surjective because for any $(ag) \cdot x \in G \cdot y$, we can recover the $g \cdot x \in G \cdot x$. Thus, φ is a bijective map, so the two groups have the same cardinality.

□