Homework 5

Aleck Zhao

October 13, 2016

Section 2.4: Cyclic Groups and the Order of an Element

4. In each case determine whether G is cyclic.

   (a) $G = \mathbb{Z}_7^*$

   Solution. Here, $G = \{1, 2, 3, 4, 5, 6\}$, where these are understood to be the equivalence classes, and the operation is multiplication. Then we have

   $$\begin{aligned} 1 &\equiv 1 \\ 2 &\equiv 3^2 \\ 3 &\equiv 3^1 \\ 4 &\equiv 3^4 \\ 5 &\equiv 3^5 \\ 6 &\equiv 3^3 \end{aligned}$$

   so $G = \langle 3 \rangle$, and $\boxed{G \text{ is cyclic.}}$

   □

   (b) $G = \mathbb{Z}_{12}^*$

   Solution. Here, $G = \{1, 5, 7, 11\}$, where these are understood to be equivalence classes, so the order of G is 4. However, $\langle 5 \rangle = \{1, 5\}$ and $\langle 7 \rangle = \{1, 7\}$, and these subgroups both have order 2, so $\boxed{G \text{ is not cyclic.}}$

   □

   (c) $G = \mathbb{Z}_{16}^*$

   Solution. Here, $G = \{1, 3, 5, 7, 9, 11, 13, 15\}$ so the order of G is 8. Now, we have

   $$\begin{aligned} \langle 3 \rangle &= \{1, 3, 9, 11\} \\ \langle 5 \rangle &= \{1, 5, 9, 13\} \end{aligned}$$

   so G has two distinct subgroups of order 4, so $\boxed{G \text{ is not cyclic.}}$

   □

(d) $G = \mathbb{Z}_{11}^*$

Solution. Here, $G = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, and we have

$$\begin{aligned} 1 &\equiv 1 \\ 2 &\equiv 2^1 \\ 3 &\equiv 2^8 \\ 4 &\equiv 2^2 \\ 5 &\equiv 2^4 \\ 6 &\equiv 2^9 \\ 7 &\equiv 2^7 \\ 8 &\equiv 2^3 \\ 9 &\equiv 2^6 \\ 10 &\equiv 2^5 \end{aligned}$$

so $G = \langle 2 \rangle$ so $\boxed{G \text{ is cyclic.}}$

□

20. (a) Find three elements of $C_6 \times C_{15}$ of maximum order.

Solution. Let $C_6 = \left\{1, g, \cdots, g^5\right\}$ and $C_{15} = \left\{1, f, \cdots, f^{14}\right\}$. Then the element of max order in C_6 is g^5, where $o(g^5) = 6$ since 5 and 6 are relatively prime. Similarly, the elements of max order in C_{15} are the elements f^k where k is relatively prime to 15, which are $k = 7, 11, 13$. Then the elements in $C_6 \times C_{15}$ of max order are

$$\boxed{(g^5, f^7), \quad (g^5, f^{11}), \quad (g^5, f^{13})}$$

which all have order $\text{lcm}(6, 15) = 30$.

□

(b) Find one element of maximum order in $C_m \times C_n$.

Solution. If $C_m = \langle g \rangle$ and $C_n = \langle f \rangle$ then we are guaranteed $o(g^{m-1}) = m$ and $o(f^{n-1}) = n$ since $m - 1$ and $n - 1$ are relatively prime to m and n, respectively. Thus, the element $\boxed{(g^{m-1}, f^{n-1})}$ is of maximum order $\text{lcm}(m, n)$.

□

28. Let H be a subgroup of a group G and let $a \in G, o(a) = n$. If m is the smallest positive integer such that $a^m \in H$, show that $m|n$.

Proof. We know that $0 \leq m \leq n - 1$, so suppose $n = qm + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r \leq m - 1$. Then

$$a^n = a^{qm+r} = a^r (a^m)^q = 1_G.$$

Since $a^m \in H$, by induction $(a^m)^q \in H$ for any $q \geq 1$, and the inverse $((a^m)^q)^{-1} \in H$ as well since H is a subgroup. However, from above, we know this inverse is exactly a^r, which must exist in H. However, since by assumption, m is the smallest positive integer such that a^m is in H, so it must be the case that $r = 0$, so $a^r = 1_G$. Thus, $n = qm$, so $m|n$, as desired.

□

Section 2.5: Homomorphisms and Isomorphisms

3. If G is any group, define $\alpha : G \to G$ by $\alpha(g) = g^{-1}$. Show that G is abelian if and only if α is a homomorphism.

Proof. If G is abelian, then $gf = fg$ for any $f, g \in G$. Then $\alpha(gf) = \alpha(fg) = (fg)^{-1} = g^{-1}f^{-1} = \alpha(g)\alpha(f)$ so $\alpha(gf) = \alpha(g)\alpha(f)$, so α is a homomorphism, as desired.

If α is a homomorphism, then $\alpha(fg) = \alpha(f)\alpha(g)$ for all $f, g \in G$. Then $(fg)^{-1} = f^{-1}g^{-1} = (gf)^{-1}$ so in fact $fg = gf$ since inverses are unique, and G is abelian, as desired.

□

6. Show that there are exactly two homomorphisms $\alpha : C_6 \to C_4$.

Proof. Let $C_6 = \{1, g, \cdots, g^5\}$ and $C_4 = \{1, f, f^2, f^3\}$. Then since $C_6 = \langle g \rangle$, a homomorphism is uniquely determined by where g is mapped to. Clearly $\alpha_1(g) = 1$ works, then α_1 maps all elements of C_6 to 1, which is a homomorphism.

Then, the mapping $\alpha_2(g) = f^2$ also determines a homomorphism. Then $\alpha_2(1) = \alpha_2(g^2) = \alpha_2(g^4) = 1$ and $\alpha_2(g) = \alpha_2(g^3) = \alpha_2(g^5) = f^2$. It's easy to check that $\alpha_2(ab) = \alpha_2(a)\alpha_2(b)$ for any $a, b \in C_6$.

Consider the mapping $\alpha_3(g) = f$. Then $\alpha_3(g^2) = f^2$ and $\alpha_3(g^3) = f^3$ and $\alpha_3(g^4) = 1$. This is a problem because $\alpha_3(g^2g^4) = \alpha_3(g^6) = \alpha_3(1) = 1$, but $\alpha_3(g^2)\alpha(g^4) = f^2 \cdot 1 = f^2$, so α_3 is not a homomorphism.

Similarly, the mapping $\alpha_4(g) = f^3$ encounters the same problems. Then $\alpha(g^5) = f^3$, so $\alpha_4(gg^5) = \alpha_4(1) = 1$ but $\alpha_4(g)\alpha_4(g^5) = f^3 \cdot f^3 = f^2$, so α_4 is not a homomorphism.

Thus, there are only two homomorphisms from C_6 to C_4, as desired.

□

13. Show that $G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\}$ is a subgroup of $GL_2(\mathbb{Z})$ isomorphic to $\{1, -1, i, -i\}$.

Proof. We first show that G is a subgroup. Here, $1_G = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity in $GL_2(\mathbb{Z})$. Then we have

$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in G$$
$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in G$$
$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$$

We can also find each element's inverse. From above, we have $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ are inverses of each other, and $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}^{-1} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$. Thus, G is indeed a subgroup.

If we define the mapping $\alpha : G \to \{1, -1, i, -i\}$ such that

$$\alpha\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) = 1 \qquad \alpha\left(\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\right) = -1$$
$$\alpha\left(\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\right) = i \qquad \alpha\left(\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\right) = -i$$

it's clear that α is surjective and injective, and it satisfies the properties of a group homomorphism (easy to check). The inverse is just the same mapping in the other direction, so G is isomorphic to $\{1, -1, i, -i\}$ as desired.

□

25. Are the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ isomorphic?

Proof. Suppose there exists an isomorphism $\varphi : \mathbb{Q} \to \mathbb{Z}$. Then since φ is surjective, there exists a $q \in \mathbb{Q}$ such that $\varphi(q) = 1$. Now consider $\varphi(q/2) + \varphi(q/2)$. Since φ is a group homomorphism, this must equal $\varphi(q/2 + q/2) = \varphi(q) = 1$. However, the equation $2\varphi(q/2) = 1$ has no solution since $\varphi(q/2) \in \mathbb{Z}$, Thus, there is no isomorphism from $\mathbb{Q}$ to $\mathbb{Z}$, so the two groups are not isomorphic.

□

33. If $Z(G) = \{1\}$, show that $G \cong \text{inn}G$.

Proof. Define the mapping $\varphi : G \to \text{inn}G$ such that $a \mapsto \sigma_a$ for all $a \in G$ where $\sigma_a(g) = aga^{-1}$ for all $g \in G$. Clearly, φ is surjective by the way we've defined it. To show φ is injective, suppose $\varphi(a) = \varphi(b)$, so that $\sigma_a = \sigma_b$. That means

$$\sigma_a(g) = aga^{-1} = bgb^{-1} = \sigma_b(g)$$

for all $g \in G$. Manipulating, we have

$$\begin{aligned} aga^{-1} &= bgb^{-1} \\ ag &= bgb^{-1}a \\ (b^{-1}a)g &= g(b^{-1}a) \end{aligned}$$

and since $Z(G) = \{1\}$, it must be that $b^{-1}a = 1$, so $b = a$, thus φ is injective.

Now, we must show φ is a homomorphism. We have

$$\varphi(a)\varphi(b) = \sigma_a\sigma_b$$

and we must show this is equal to

$$\varphi(ab) = \sigma_{ab}.$$

That is, we must show

$$\sigma_a(\sigma_b(g)) = \sigma_{ab}(g)$$

for all $g \in G$. This is

$$\begin{aligned} \sigma_a(\sigma_b(g)) &= \sigma_a(bgb^{-1}) \\ &= abgb^{-1}a^{-1} \\ &= (ab)g(ab)^{-1} \\ &= \sigma_{ab}(g) \end{aligned}$$

so $\sigma_a\sigma_b = \sigma_{ab}$ and φ is a homomorphism.

Combining these, we have φ is an isomorphism, so $G \cong \text{inn}G$, as desired.

□

Section 2.6: Cosets and Lagrange's Theorem

1. In each case find the right and left cosets in G of the subgroups H and K of G.

   (e) $G = D_4 = \left\{1, a, a^2, a^3, b, ba, ba^2, ba^3\right\}$, $o(a) = 4, o(b) = 2$, and $aba = b$; $H = \left\langle a^2 \right\rangle, K = \langle b \rangle$.

   Solution. We have $H = \left\{1, a^2\right\}$, so the left cosets of H in G are given by

   $$\begin{aligned} 1H &= \left\{1, a^2\right\} \\ aH &= \left\{a, a^3\right\} \\ bH &= \left\{b, ba^2\right\} \\ (ba)H &= \left\{ba, ba^3\right\} \end{aligned}$$

   and the right cosets of H in G are

   $$\begin{aligned} H1 &= \left\{1, a^2\right\} \\ Ha &= \left\{a, a^3\right\} \\ Hb &= \left\{b, a^2b\right\} = \left\{b, ba^2\right\} \\ H(ba) &= \left\{ba, a^2ba\right\} = \left\{ba, ba^3\right\} \end{aligned}$$

   We have $K = \{1, b\}$ so the left cosets of K in G are given by

   $$\begin{aligned} 1K &= \{1, b\} \\ aK &= \{a, ab\} = \left\{a, ba^3\right\} \\ (a^2)K &= \left\{a^2, a^2b\right\} = \left\{a^2, ba^2\right\} \\ (a^3)K &= \left\{a^3, a^3b\right\} = \left\{a^3, ba\right\} \end{aligned}$$

   and the right cosets of K in G are

   $$\begin{aligned} K1 &= \{1, b\} \\ Ka &= \{a, ba\} \\ K(a^2) &= \left\{a^2, ba^2\right\} \\ K(a^3) &= \left\{a^3, ba^3\right\} \end{aligned}$$

   □

   (f) $G =$ any group; H is any subgroup of index 2.

   Solution. Since the index of H in G is 2, there are two distinct cosets. Clearly $H1 = 1H = H$ is a coset, and since cosets are disjoint and partition G, the other coset is exactly $G \setminus H$. In this case, the left and right cosets are the same.

   □

17. Let $|G| = p^2$, where p is a prime. Show that every proper subgroup of G is cyclic.

   Proof. By Lagrange's Theorem, if H is a subgroup, then $|H|$ divides $|G|$, so $|H| = 1, p, p^2$. The proper subgroups are where $|H| = p$. By Corollary 3, H is necessarily cyclic, as desired.

   □