

Math 113 Homework 4 Solutions

Rather than repeating the same argument in several problems, here is a general version:

Lemma 1. *If G is a finite abelian group, p is a prime, and G has at least p elements of order p , then p^2 divides the order of G*

Proof: *If $g \in G$ is an element of order p , then $\langle g \rangle$ has $p - 1$ elements of order p . If there are at least p of order p , then there is one not in $\langle g \rangle$, call it h . Since g and h are order p , $\langle g \rangle$ and $\langle h \rangle$ are each generated by any element except the identity. As $\langle g \rangle \neq \langle h \rangle$, it must be that $\langle g \rangle \cap \langle h \rangle = \{e\}$. Consider $K = \{g^i h^k\} = \langle g \rangle \langle h \rangle$. Since G is abelian, $g^{i_1} h^{j_1} g^{i_2} h^{j_2} = g^{i_1+i_2} h^{j_1+j_2}$. Also $g^0 h^0 = e$ and $(g^i h^j)^{-1} = g^{-i} h^{-j}$. So K is a subgroup of G . As G is abelian, K is the internal direct product of $\langle g \rangle$ and $\langle h \rangle$. So K has p^2 elements. Since K is a subgroup of G , by Lagrange's Theorem p^2 divides the order of G .*

(1) Do exercise 4.29 in Judson.

Recall that for a reflection s and a smallest rotation r , D_n consists of things of the form r^i and sr^i . Since $n \geq 3$, $r \neq r^{-1}$. Now for any i ,

$$(sr^i)(sr^{i+1}) = s(sr^{-i})r^{i+1} = r \neq r^{-1} = s(sr^{-i-1})r^i = (sr^{i+1})(sr^i)$$

So sr^i is never in the center. As for r^i , we know $r^i s = sr^{-i}$. For $r^i = r^{-i}$, we need to have $i \equiv -i \pmod{n}$. So the only possibilities for i are 0 and $\frac{n}{2}$. r^0 is just the identity, which is always in the center. If n is even, $r^j r^{n/2} = r^{j+n/2} = r^{n/2} r^j$ and $r^{n/2} (sr^j) = sr^{-n/2} r^j = sr^{n/2} r^j = (sr^j) r^{n/2}$. So if n is odd, the $Z(D_n)$ is trivial. If n is even $Z(D_n)$ is the identity and the 180° rotation.

(2) Do exercise 5.10 in Judson.

For each $b \in \mathbb{R}$, $bi + \mathbb{R}$ is a different coset. This is because if $b_1 i + a_1 = b_2 i + a_2$ then $b_1 = b_2$ and $a_1 = a_2$. Since each real b gives a distinct coset, and there are infinitely many reals, we get infinitely many distinct cosets. So $[\mathbb{C}, \mathbb{R}]$ is infinite.

(3) Do exercise 5.19 in Judson.

We'll prove $gH \cap gK = g(H \cap K)$. For any $x \in G$:

$$\begin{aligned} x \in gH \cap gK &\iff x \in gH \text{ and } x \in gK \iff \text{there are } h \in H, k \in K, x = gk = gh \\ &\iff \text{there is } a \in H \cap K, x = ga \iff x \in g(H \cap K) \end{aligned}$$

The third step works because if $x = gh = gk$, then $h = k$ by left cancellation.

(4) Give an example of a group G , a subgroup H , and $a, b \in G$, so that $aH = bH$ but $Ha \neq Hb$.

Take $G = S_3$, $H = \{id, (1\ 2)\}$, $a = (1\ 3)$, and $b = (1\ 2\ 3)$. Then we get

$$(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\} = (1\ 2\ 3)H$$

$$H(1\ 3) = \{(1\ 3), (1\ 3\ 2)\} \neq \{(1\ 2\ 3), (2\ 3)\} = H(1\ 2\ 3)$$

(5) Do exercise 8.8 in Judson

We know \mathbb{Z} is cyclic, specifically $\mathbb{Z} = \langle 1 \rangle$. We'll show that \mathbb{Q} is not cyclic, so it is impossible for \mathbb{Z} and \mathbb{Q} to be isomorphic. Pick any $q \in \mathbb{Q}$. Then $\frac{q}{2} \notin \langle q \rangle$. So $\mathbb{Q} \neq \langle q \rangle$. Thus \mathbb{Q} is not generated by any single $q \in \mathbb{Q}$, i.e. it is not cyclic.

(6) (a) If G is a group of size 4, prove that G is isomorphic to either \mathbb{Z}_4 or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Recall that the order of an element always divides the order of a group. So each element of G must have order 1, 2, or 4. If G has any element g of order 4, then $G = \langle g \rangle$. So G would be cyclic and thus isomorphic to \mathbb{Z}_4 .

Now consider the case that G has no elements of order 4. I.e. all elements are order 1 or 2. The only element of order 1 is the identity. So $G = \{e, a, b, c\}$ where e is the identity and a, b, c are all order 2. Since a, b, c all have order 2, $a^2 = b^2 = c^2 = e$, and every element of the group is its own inverse.

Now consider ab . ab cannot be e , because then $b = a^{-1} = a$. Also if $ab = a$ then $b = e$ and if $ab = b$ then $a = e$. So it must be that $ab = c$. By the same argument, we get $ba = c$, $ac = b = ca$, and $bc = a = cb$. We now know the entire Cayley table of G . Define a function $f : G \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ defined by $f(e) = (0, 0)$, $f(a) = (0, 1)$, $f(b) = (1, 0)$, and $f(c) = (1, 1)$. f is bijective since there is a correspondence between the domain and codomain. And we can verify f is a homomorphism by checking that for each pair of elements $x, y \in G$, $f(xy) = f(x) + f(y)$.

(b) If G is a group of size 6, prove that G is isomorphic to either \mathbb{Z}_6 or S_3 .

We know that the possible orders of elements of G are 1, 2, 3, and 6, because they must divide the order of G .

First consider the case that G is abelian. In this case, note that $2^2 = 4$ and $3^2 = 9$ do not divide 6. So by Lemma 1, G has at most one element of order 2, and at most 2 elements of order 3. Since the only element of order 1 is the identity, this leaves 2 elements which must be of order 6. Any element of order 6 must generate G , so G is cyclic and must be isomorphic to \mathbb{Z}_6 .

Now consider the case that G is not abelian. If G had a element of order 6, G would be cyclic and thus abelian. So G can only have elements of order 1, 2, and 3. If G had only elements of order 1 and 2, by problem 7 on Exam 1, G would be abelian. So G must have an element of order 3, call it g . Now $\langle g \rangle$ has size 3. So we can pick some h in $G \setminus \langle g \rangle$. Since $\langle g \rangle$ has size 3, by Lagrange's theorem the index of $\langle g \rangle$ in G , $[G : \langle g \rangle]$, must be 2. So the left cosets of $\langle g \rangle$ are just $\langle g \rangle$ and $G \setminus \langle g \rangle = h \langle g \rangle$. In other words $G = \langle g \rangle \cup h \langle g \rangle = \{e, g, g^2, h, hg, hg^2\}$.

Consider gh . We'll show $gh = hg^2$. If $gh = g^i$, then $h = g^{i-1}$. But $h \notin \langle g \rangle$. So $gh \neq g^i$ for any i . If $gh = h$, then $g = e$, which is not possible. So $gh \neq h$. Finally, if $gh = hg$, then all elements of G would commute. But G is not abelian, so $gh \neq hg$. Thus $gh = hg^2$. This tells us $g^i h g^j = h g^{j-1}$, and we can now compute the entire Cayley table of G . This allows us to verify that the

bijection $f : G \rightarrow S_3$ defined by:

$$\begin{aligned} f(e) &= id & f(h) &= (1\ 2) \\ f(g) &= (1\ 2\ 3) & f(hg) &= (2\ 3) \\ f(g^2) &= (1\ 3\ 2) & f(hg^2) &= (1\ 3) \end{aligned}$$

is a homomorphism. So G and S_3 are isomorphic.

(7) (a) Do exercise 8.24 in Judson.

Let G be an abelian group of order $51 = 3 \cdot 17$. So the possible orders of elements are 1, 3, 17, and 51. There's only 1 element of order 1. Neither 3^2 nor 17^2 divides 51. So by Lemma 1, there are at most 2 elements of order 3, and at most 16 elements of order 17. So there have to be at least $51 - 1 - 2 - 16 = 32$ elements of order 51. Any element of order 51 generated G , So G must be cyclic.

(b) Do exercise 8.25 in Judson.

Consider $G = \mathbb{Z}_2 \times \mathbb{Z}_{26}$. For any $(a, b) \in G$, $(a, b)^{26} = (26a, 26b) = (0, 0)$. So every element of G has order at most 26 and G cannot be cyclic.

(8) For an abelian group G , we define $\mathbb{Z}_2 \times G$ to be the set $\{[0], [1]\} \times G$ with the operation

$$([i], x) \cdot ([j], y) = ([i + j], x^{(-1)^j} y)$$

(a) Prove that this operation is well defined and that $\mathbb{Z}_2 \times G$ is a group.

First we'll prove associativity. Let $([a_1], x_1), ([a_2], x_2), ([a_3], x_3) \in \mathbb{Z}_2 \times G$. Then

$$\begin{aligned} ([a_1], x_1) \cdot (([a_2], x_2) \cdot ([a_3], x_3)) &= ([a_1], x_1) \cdot ([a_2 + a_3], x_2^{(-1)^{a_3}} x_3) \\ &= ([a_1 + a_2 + a_3], x_2^{(-1)^{a_2+a_3}} x_2^{(-1)^{a_3}} x_3) \end{aligned}$$

and

$$\begin{aligned} (([a_1], x_1) \cdot ([a_2], x_2)) \cdot ([a_3], x_3) &= ([a_1 + a_2], x_1^{(-1)^{a_2}} x_2) \cdot ([a_3], x_3) \\ &= ([a_1 + a_2 + a_3], (x_1^{(-1)^{a_2}} x_2)^{(-1)^{a_3}} x_3) \\ &= ([a_1 + a_2 + a_3], x_2^{(-1)^{a_2+a_3}} x_1^{(-1)^{a_3}} x_3) \end{aligned}$$

The last equality is true because G is commutative. Now we'll prove $([0], e_G)$ is the identity of $\mathbb{Z}_2 \times G$. Let $([i], x)$ be any element of $\mathbb{Z}_2 \times G$. Then:

$$([0], e_G) ([i], x) = ([0 + i], e_G^{(-1)^i} x) = ([i], x) = ([i + 0], x^{(-1)^0} e_G) = ([i], x) ([0], e_G)$$

Finally, we'll check that $([i], x)^{-1} = ([i], x^{(-1)^i})$:

$$([i], x) ([i], x^{(-1)^{i+1}}) = ([2i], x^{(-1)^i} x^{(-1)^{i+1}}) = ([0], x^{(-1)^i(1-1)}) = ([0], e_G)$$

and

$$([i], x^{(-1)^{i+1}}) ([i], x) = ([2i], (x^{(-1)^{i+1}}) x) = ([0], x^{(-1)^{2i+1}}) = ([0], x^{-1}x) = ([0], e_G)$$

So $\mathbb{Z}_2 \times G$ is a group.

(b) Prove that for $n \geq 3$, $\mathbb{Z}_2 \times \mathbb{Z}_n$ is isomorphic to D_n .

Pick s a reflection in D_n and r a smallest rotation. Recall that $D_n = \{r^i, sr^i\}$ and $sr^i = r^{-i}s$. Define $f : \mathbb{Z}_2 \times \mathbb{Z}_n \rightarrow D_n$ by $f([i]_2, [j]_n) = s^i r^j$. First we need to check that f is well defined. If $[i_1]_2 = [i_2]_2$ and $[j_1]_n = [j_2]_n$, then $i_1 = i_2 + 2k$ and $j_1 = j_2 + ln$. So

$$s^{i_1} r^{j_1} = s^{i_2+2k} r^{j_2+ln} = s^{i_2} (s^2)^k r^{j_2} (r^n)^l = s^{i_2} r^{j_2}$$

and f is well defined. Now we can check that f is a homomorphism:

$$f((i, j)(0, j')) = f((i, j + j')) = s^i r^{j+j'} = (s^i r^j) r^{j'} = f((i, j))f((0, j'))$$

and

$$f((i, j)(1, j')) = f((i+1, -j+j')) = s^{i+1} r^{-j+j'} = s^i (sr^{-j}) r^{j'} = s^i r^j sr^{j'} = f((i, j))f((1, j'))$$

To show that f is injective, suppose $f((i_1, j_2)) = f((i_2, j_2))$. Then $s^{i_1} r^{j_1} = s^{i_2} r^{j_2}$. Which tells us that $s^{i_1-i_2} = r^{j_2-j_1}$. That's only possible if both are the identity. In that case $i_1 \equiv i_2 \pmod{2}$ and $j_1 \equiv j_2 \pmod{n}$. So f is injective. And f must be surjective since $s^i r^j = f((i, j))$. So f is an isomorphism from $\mathbb{Z}_2 \times \mathbb{Z}_n$ to D_n .

(9) Do exercise 8.29 in Judson.

We will define a map $f : S_n \rightarrow A_{n+2}$ and prove that it is an injective homomorphism. Thus f will be an isomorphism between S_n and the range of A_{n+2} .

$$f(\sigma) = \begin{cases} \sigma & \text{if } \sigma \text{ is even} \\ \sigma \cdot (n+1 \ n+2) & \text{if } \sigma \text{ is odd} \end{cases}$$

In both cases, $f(\sigma)$ is even and so in A_{n+2} . Since $(n+1 \ n+2)$ and σ are disjoint, they commute. Using this, f is easily checked to be a homomorphism. To see that f is injective, suppose $\tau = f(\sigma_1) = f(\sigma_2)$. If $\tau(n+1) = n+1$, then both σ_1 and σ_2 are even and so must be equal. If $\tau(n+1) \neq n+1$, then both are odd, and again must be equal. So f is injective and as desired.

(10) Let G be a group and let $f : G \rightarrow G$ be the function $f(x) = x^{-1}$. Prove that f is an isomorphism if and only if G is abelian.

First notice that f is its own inverse, so it's always bijective.

If f is an isomorphism, then for any x and y in G ,

$$xy = f(f(xy)) = f(f(x)f(y)) = f(x^{-1}y^{-1}) = (x^{-1}y^{-1})^{-1} = (y^{-1})^{-1} (x^{-1})^{-1} = yx$$

So G is abelian.

In the other direction, if G is abelian, then

$$f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y)$$

so f is a homomorphism. And we already know f is bijective, so it's an isomorphism.