

HW 1 Solutions

April 18, 2009

Exercise 1.6 Problem 2: If $\phi : G \rightarrow H$ is an isomorphism, prove that $|\phi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is the result true if ϕ is only assumed to be a homomorphism?

Solution: First things first, the result is **patently false** if ϕ is only assumed to be a homomorphism. For instance, G can be any group you like, with all kinds of elements of all kinds of orders, and you can take H to be the trivial group and ϕ the trivial homomorphism which maps every element in G to the identity element of H .

With that out of the way, let's prove the first statement of this problem. Notice that $(\phi(x))^{|x|} = \phi(x^{|x|}) = \phi(1) = 1$. The first equality follows from the repeated application of the homomorphism identity, and the second equality follows by the definition of the order. This shows that $|\phi(x)| \leq |x|$. Now we use a "trick" to show that $|x| \leq |\phi(x)|$. Recall that if ϕ is a group isomorphism, then ϕ has an inverse map, ϕ^{-1} , and that ϕ^{-1} is also a group isomorphism. Repeat the argument above replacing the element x by the element $\phi(x)$ and let the isomorphism under consideration be ϕ^{-1} . The argument tells us that $|\phi^{-1}(\phi(x))| \leq |\phi(x)|$. But $\phi^{-1}(\phi(x))$ is of course the same element as x , so the inequality then reads $|x| \leq |\phi(x)|$. The only way the two inequalities $|x| \leq |\phi(x)|$ and $|\phi(x)| \leq |x|$ can hold is for $|x| = |\phi(x)|$.

Now we must deduce that any two isomorphic groups G and H have the same number of elements of a given order n . Let G_n denote the subset of G consisting of all elements of order n and let H_n denote the subset of H consisting of all elements of order n . Suppose ϕ is an isomorphism between G and H . Let ϕ_n denote the restriction of ϕ to the domain G_n .

The paragraph above shows that the image of ϕ_n lies in H_n . We claim that this is a bijection of sets (or in other words, G_n and H_n have the same cardinality). As ϕ is injective, its restriction is too. It only remains to show that $\phi_n : G_n \rightarrow H_n$ is onto. Let $h \in H_n$. Then by the paragraph above we know that $\phi^{-1}(h)$ also has order n , so it must be an element of G_n . Then $\phi_n(\phi^{-1}(h)) = \phi(\phi^{-1}(h)) = h$. This proves that ϕ_n is onto and hence a bijection between G_n and H_n . This means that that G and H have the same number of elements of order n .

Exercise 1.6 Problem 6: Prove that the additive groups \mathbb{Z} and \mathbb{Q} are not isomorphic.

Solution: The group \mathbb{Z} enjoys the property that it is *cyclic*. This means there there is an element $z \in \mathbb{Z}$ such that every other element of \mathbb{Z} is equal to z^n for some $n \in \mathbb{Z}$. The element z in this case is either -1 or 1 (a little confusion here. 1 is NOT the identity element in \mathbb{Z} , 0 is the identity element. Also, as \mathbb{Z} is an additive group, z^n means $z + \dots + z$ which we will write as nz .) The group \mathbb{Q} is not cyclic. If it were, then it would have an element z whose positive and negative powers generated all elements of \mathbb{Q} . In particular, z would have to be nonzero, and as such, we could consider $\frac{z}{2}$. If there were an integer $n \in \mathbb{Z}$ such that $\frac{z}{2} = nz$ then we'd have $(n - \frac{1}{2})z = 0$. As $z \neq 0$ this would imply that $n - \frac{1}{2} = 0$ which in turn would say that $n = \frac{1}{2}$. But $\frac{1}{2}$ is not an integer. So \mathbb{Q} is not cyclic. We conclude the problem by showing the following lemma.

Lemma 0.1. *if $\phi : G \rightarrow H$ is an isomorphism and G is cyclic, then H is cyclic too.*

As G is cyclic, it has an element x whose positive and negative powers generate all the elements of G . We claim that the positive and negative powers of $\phi(x)$ generate all the elements of H , hence H is cyclic. Let $h \in H$. As ϕ is an isomorphism, it is onto. So there is an element $g \in G$ such that $\phi(g) = h$. As G is cyclic, $g = x^n$ for some $n \in \mathbb{Z}$. Then $\phi(x)^n = \phi(x^n) = \phi(g) = h$. So $\phi(x)$ generates all the elements of H , hence H is cyclic.

\mathbb{Z} and \mathbb{Q} can't be isomorphic because if they were, the lemma would prove that \mathbb{Q} was cyclic which is a contradiction.

Exercise 1.6 Problem 7: Prove that D_8 and Q_8 are not isomorphic.

Solution: This is an excellent time to use the results we showed in Exercise 1.6 Problem 2. If D_8 and Q_8 were isomorphic they'd have the same number of elements of a given order. However Q_8 has six elements of order 4 (i,j,k,-i,-j,-k) while D_8 has only two (rotation by 90° and by 270°).

Exercise 1.6 Problem 17: Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.

Solution: \Rightarrow Suppose this map, which we'll call ϕ , is a homomorphism and x and y are elements of G . Then we have

$$\phi(xy) = \phi(x)\phi(y).$$

By the definition of ϕ , this equation is equivalent to

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

Multiply this equation on both sides by xy on the left and yx on the right to obtain

$$\begin{aligned} (xy)(xy)^{-1}(yx) &= (xy)x^{-1}y^{-1}(yx) \\ yx &= (xy)x^{-1}y^{-1}(yx). \end{aligned}$$

Now we regroup the righthand side using the associative law

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

So $yx = xy$. As x and y were arbitrary, we conclude that G is abelian.

\Leftarrow Suppose G is abelian. Then

$$\phi(x)\phi(y) := x^{-1}y^{-1}.$$

Because G is abelian this is equal to

$$\begin{aligned} &= y^{-1}x^{-1} \\ &= (xy)^{-1} := \phi(xy). \end{aligned}$$

Exercise 1.6 Problem 26: Let i and j be the generators of Q_8 described in Section 5. Prove that the map ϕ from Q_8 to $GL_2(\mathbb{C})$ defined on generators by

$$\phi(i) = \begin{bmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{bmatrix} \text{ and } \phi(j) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

extends to a homomorphism. Prove that ϕ is injective.

Solution: I will try to present the solution in a systematic way. It hinges on a lemma

Lemma 0.2. *Let G be a group with group presentation $\langle a, b \mid r_1(a, b) = \dots = r_l(a, b) = 1 \rangle$ where the $r_i(a, b)$ are words in a and b . Also suppose we have a group H and a function ϕ which is defined only on the set $\{a, b\}$. Let $w = a^{n_1} b^{m_1} \dots a^{n_k} b^{m_k}$ be a word. We will call (for this exercise only) the element $\phi(a)^{n_1} \phi(b)^{m_1} \dots \phi(a)^{n_k} \phi(b)^{m_k}$ the forced extension of ϕ to the word w . If the forced extensions of ϕ to all of the words $r_1(a, b), \dots, r_l(a, b)$ are all equal to the identity element of H , then ϕ extends to a homomorphism on G . (By the way, this lemma is true for groups generated by more than two elements...but well, for simplicity's sake...)*

Before proving the lemma, let's see how it helps us solve the problem. You may/should check that the quaternion group Q_8 has presentation

$$\langle i, j \mid i^4 = j^4 = i^2 j^2 = i j i^{-1} j = 1 \rangle.$$

You may also check on your own time that the forced extension of ϕ to the words $i^4, j^4, i^2 j^2$, and $i j i^{-1} j$ is the identity matrix. For example the forced extension to $i^2 j^2$ is

$$\begin{aligned} & \begin{bmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{bmatrix}^2 \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^2 \\ &= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \end{aligned}$$

The lemma then tells us that ϕ extends to a homomorphism to all of Q_8 . Now we must prove the lemma. It is harder than the rest of the solutions, and you shouldn't feel bad about skipping it.

Proof. In this proof we will construct an extension of ϕ to the group generated by a and b . We will call this extension ϕ_{ex} . First we must note two things. First, recall that an element $x \in G$ is actually an equivalence class of words, where two words w and w' are equivalent if there is a sequence of words v_1, \dots, v_s , each a relation of G or an inverse of one, such

that $w' = v_1 \cdots v_s w$. At this point, let's give the forced extension of a word g by ϕ a name: $\phi_F(g)$. The second thing to note (check this!) is that whenever we have two words g and h we have the relation that $\phi_F(gh) = \phi_F(g)\phi_F(h)$. Also you may/should check that if g is a word and g^{-1} is its inverse word, then $\phi_F(g^{-1}) = \phi_F(g)^{-1}$. In particular, if $\phi_F(g)$ happens to be the identity, then so is $\phi_F(g^{-1})$. Ok, these preliminaries aside, we may proceed.

Let w be a word in the equivalence class x . We define $\phi_{ex}(x)$ to be the element $\phi_F(w)$. Now why is this well defined? Isn't it conceivable that if we pick a different word w' in the equivalence class x that the forced extension of ϕ to w' will not be the same as the forced extension of ϕ to w ? Well, we'll show that under the hypothesis of the lemma that it won't matter which choice of representing word we pick; its forced extension by ϕ is the same. To that end, if w and w' both lie in the same equivalence class x , then by definition of these equivalence classes, there is a sequence of words v_1, \dots, v_s such that $w' = v_1 \cdots v_s w$ and all the v_i (or their inverses) are words appearing in the relations $r_1(a, b), \dots, r_s(a, b)$ used to present G .

Now we can examine the forced extension of w' .

$$\phi_F(w') = \phi_F(v_1) \cdots \phi_F(v_s) \phi_F(w)$$

where we've applied the relation $\phi_F(gh) = \phi_F(g)\phi_F(h)$ s times. Now $\phi_F(v_i) = 1$ because each word v_i , or its inverse, came from the list of relations and by hypothesis $\phi_F(r_j(a, b)) = 1$ for any relation (or its inverse by our second note). Thus our equation simplifies to

$$= 1 \cdots 1 \phi_F(w) = \phi_F(w).$$

So it did not matter which word we picked in the equivalence class x . Any two words had the same forced extension to ϕ . So the definition

$$\begin{aligned} \phi_{ex} : G &\longrightarrow H \\ x &\longmapsto \phi_F(w) \end{aligned}$$

where w is a word in the equivalence class of x , does define a valid function.

It remains to show that ϕ_{ex} is a group homomorphism. Let x and y be elements of G , and let w_1 and w_2 be words in those respective equivalence classes. Then $w_1 w_2$ is a word in the equivalence class xy . We then have

$$\phi_{ex}(x)\phi_{ex}(y) = \phi_F(w_1)\phi_F(w_2) = \phi_F(w_1 w_2) := \phi_{ex}(xy).$$

So ϕ_{ex} is a group homomorphism defined on G which extends ϕ . □

Exercise 1.7 Problem 8: Let A be a nonempty set and let k be a positive integer with $k \leq |A|$. The symmetric group S_A (defined as the set of all bijections of A to itself) acts on the set B consisting of all subsets of A of cardinality k by $\sigma \cdot \{a_1, \dots, a_k\} = \{\sigma(a_1), \dots, \sigma(a_k)\}$.

- (a) Prove that this is a group action
 (b) Describe explicitly how the elements $(1\ 2)$ and $(1\ 2\ 3)$ act on the six 2-element subsets of $\{1, 2, 3, 4\}$.

Solution:

- (a) If $\{a_1, \dots, a_k\}$ is a set with cardinality k , then $\{\sigma(a_1), \dots, \sigma(a_k)\}$ is too because $\sigma \in S_A$ is a bijection and in particular one-to-one. So the definition of σ acting on B does take values in B . It remains to verify the two criteria for a group action: (1) $\sigma_1 \cdot (\sigma_2 \cdot a) = (\sigma_1 \sigma_2) \cdot a$ for all $\sigma_1, \sigma_2 \in S_A$ and $a \in B$.
 (2) $1 \cdot a = a$ for all $a \in B$.

Towards the first criterion, let $\sigma_1, \sigma_2 \in S_A$ and $a = \{a_1, \dots, a_k\} \in B$. Then

$$\begin{aligned} \sigma_1 \cdot (\sigma_2 \cdot a) &:= \sigma_1 \cdot \{\sigma_2 a_1, \dots, \sigma_2 a_k\} \\ &= \{\sigma_1(\sigma_2 a_1), \dots, \sigma_1(\sigma_2 a_k)\}. \end{aligned}$$

Now for each of the a_i we have $\sigma_1(\sigma_2 a_i) = (\sigma_1 \sigma_2) a_i$ just for the fact that the σ 's are functions. So the set above is equal to

$$\begin{aligned} &= \{(\sigma_1 \sigma_2) a_1, \dots, (\sigma_1 \sigma_2) a_k\} \\ &:= (\sigma_1 \sigma_2) a. \end{aligned}$$

Thus we've verified the first criterion.

The second criterion follows easily because if $a = \{a_1, \dots, a_k\}$ and 1 is the identity map on A , then $1 \cdot a = \{1(a_1), \dots, 1(a_k)\} = \{a_1, \dots, a_k\} = a$. Looks like we've got ourselves a group action.

Exercise 1.7 Problem 16: Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a = gag^{-1}$ for all $g, a \in G$ do satisfy the group the asioms of a left group action (this action of G on itself is called *conjugation*).

Solution: Clearly $(g, a) \mapsto gag^{-1}$ defines a map $G \times G \rightarrow G$ because G is closed under multiplication. It remains to check that the properties of a group action are satisfied.

1) We must check that for all $g_1, g, a \in G$ that $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$. To that end,

$$\begin{aligned} g_1 \cdot (g_2 \cdot a) &= g_1 \cdot (g_2 a g_2^{-1}) \\ &= g_1 (g_2 a g_2^{-1}) g_1^{-1}. \end{aligned}$$

We regroup using the groups associative law to yield

$$= (g_1 g_2) a (g_2^{-1} g_1^{-1}).$$

Now recall that $g_2^{-1} g_1^{-1} = (g_1 g_2)^{-1}$ (because $1 = g_1 g_1^{-1} = g_1 1 g_1^{-1} = g_1 g_2 g_2^{-1} g_1^{-1}$). Plugging this in to our equation gives

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

which by definition is $(g_1 g_2) \cdot a$. 2) We must check that for all $a \in G$ that $1 \cdot a = a$. To that end,

$$1 \cdot a := 1 a 1^{-1} = 1 a 1 = a.$$

Thus we have a group action on our hands.

Exercise 1.7 Problem 18: Let H be a group acting on a set A . Prove that the relation \sim on A defined by

$$a \sim b \text{ if and only if } a = h \cdot b \text{ for some } h \in H$$

is an equivalence relation.

Solution: We must check that \sim satisfies the reflexivity, symmetry, and transitivity conditions for a relation.

Reflexivity: Notice that $a = 1 \cdot a$, so $a \sim a$.

Symmetry: If $a \sim b$, then $a = h \cdot b$ for some $h \in H$. We claim that $b = h^{-1} \cdot a$. By substituting $h \cdot b$ in for a we get

$$h^{-1} \cdot a = h^{-1} \cdot (h \cdot b).$$

We use the first property of group actions to equate the righthand side with

$$\begin{aligned} &= (h^{-1} h) \cdot b \\ &= 1 \cdot b \end{aligned}$$

which is equal to b by the second property of group actions. So $b = h^{-1} \cdot a$ which means that $b \sim a$.

Transitivity: Suppose that $a \sim b$ and $b \sim c$ for three elements a, b and c in A . This means that there are elements g and h in H such that $a = g \cdot b$ and $b = h \cdot c$. Then we may substitute $h \cdot c$ for b in the equation $a = g \cdot b$. This yields

$$a = g \cdot b = g \cdot (h \cdot c) = (gh) \cdot c.$$

But as G is a group, gh is an element of G also, so this shows that $a \sim c$.

Exercise 2.1 Problem 2: In each of (a)-(e) prove that the specified subset is *not* a subgroup of the given group:

- (a) the set of 2-cycles in S_n for $n \geq 3$.
- (b) the set of reflections in D_{2n} for $n \geq 3$.
- (c) for n a composite integer greater than one and G a group containing an element of order n , the set $\{x \in G \mid |x| = n\} \cup \{1\}$.
- (d) the set of odd integers in \mathbb{Z} together with 0.
- (e) the set of real numbers whose square is a rational number (under addition).

Solution:

(a) As n is at least 3, the 2-cycles (12) and (23) are elements in S_n . A quick check shows that $(1\ 2)(2\ 3) = (1\ 2\ 3)$. So this set is not closed under multiplication.

(b) Since $n \geq 3$, the identity is not a reflection. If the a reflection were the identity, then it would have to fix all the vertices of the n -gon. As it stands though, the only vertices a reflection fixes are the vertices that lie on the line being reflected across. The intersection of any line going through the origin with the n -gon is two points. As the n -gon has at least three vertices, one of them is not fixed by the reflection. Hence no reflection in D_{2n} acts as the identity on the n -gon.

(c) Take G to be $\mathbb{Z}/4$. The element 1 has order four hence is an element in our set, but the element $2 = 1 + 1$ has order 2. Our set is not closed under group multiplication.

(d) 1 and 3 are elements of this set. However when we multiply them together we get 4 which is not in our set.

(e) $\sqrt{2}$ and $\sqrt{3}$ are elements of our set. However $(\sqrt{2} + \sqrt{3})^2 = 2 + 3 + 2\sqrt{6}$ which is not rational. This is because $\sqrt{6}$ is not rational. If it were, there would be positive integers a and b such that $\frac{a}{b} = \sqrt{6}$ and hence $a^2 = 6b^2$. This cannot happen because of unique prime factorization. Notice that the number of 2's that factor in the square of a number is even, so the left-hand side, a^2 , has an even number of 2's in its factorization, whereas the

righthand side must have an odd number of 2's in its factorization (an even number in b^2 plus the one factor of 2 coming from $6 = 2 \cdot 3$.)

Exercise 2.1 Problem 4: Give an explicit example of a group G and an infinite subset H of G that is closed under multiplication, but is not a subgroup of G .

Solution: Let G be the integers. Let H be the natural numbers (it doesn't matter if your definition of \mathbb{N} includes 0 or not).

Exercise 2.1 Problem 9: Let $G = GL_n(F)$, where F is any field. Define

$$SL_n(F) = \{ A \in GL_n(F) \mid \det(A) = 1 \}$$

(called the *special linear group*). Prove that $SL_n(F)$ is a subgroup of $GL_n(F)$.

Solution: The identity matrix has determinant equal to 1, so $SL_n(F)$ contains it. Thus we know that $SL_n(F)$ is non-empty. Recall the rule for the determinant of a product of two matrices:

$$\det(AB) = \det(A)\det(B).$$

If A and B are elements of $SL_n(F)$, then the determinant of their product must also be equal to one because $\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$. So $SL_n(F)$ is closed under products. Lastly, we must check that $SL_n(F)$ is closed under taking inverses. So suppose that A is an element of $SL_n(F)$. Examine the determinant rule again setting $B = A^{-1}$. Then we have

$$\det(AA^{-1}) = \det(A)\det(A^{-1}).$$

As AA^{-1} is the identity matrix, this equation simplifies to

$$\det(I) = \det(A)\det(A^{-1}).$$

$$1 = \det(A)\det(A^{-1}).$$

Since A is an element of $SL_n(F)$, it must be that $\det(A) = 1$. Plugging this in to our equation yields

$$1 = 1 \cdot \det(A^{-1}) = \det(A^{-1}).$$

Thus $\det(A^{-1}) = 1$ and so A^{-1} is an element of $SL_n(F)$. We have now verified that $SL_n(F)$ is nonempty and closed under multiplication and inverses.

$SL_n(F)$ is a subgroup of $GL_n(F)$.

Exercise 2.1 Problem 12: Let A be an abelian group and fix some $n \in \mathbb{Z}$. Prove that the following sets are subgroups of A :

- (a) $S := \{ a^n \mid a \in A \}$
- (b) $T := \{ a \in A \mid a^n = 1 \}$

Solution:

(a) Since $1 = 1^n$, 1 must be an element of S , so S is nonempty. Let x and y be elements of S . We wish to show that $xy^{-1} \in S$, and the way to do this is to verify that xy^{-1} is the n^{th} power of some element of A . To that end, since x and y are elements of S there must be an element $\bar{x} \in A$ such that $x = \bar{x}^n$ and there must be an element $\bar{y} \in A$ such that $y = \bar{y}^n$. We claim that $(\overline{xy^{-1}})^n = xy^{-1}$. This is because

$$\begin{aligned}(\overline{xy^{-1}})^n &= \bar{x}^n (\bar{y}^{-1})^n \text{ (true because } A \text{ is abelian.)} \\ &= \bar{x}^n (\bar{y}^n)^{-1} \\ &= xy^{-1}.\end{aligned}$$

Thus xy^{-1} is the n^{th} power of $\overline{xy^{-1}}$ so $xy^{-1} \in S$. By the subgroup criterion, S is a subgroup of A .

(b) Since $1^n = 1$, 1 must be an element of T , so T is nonempty. Let x and y be elements of T . We wish to show that $xy^{-1} \in T$, and the way to do this is to verify that the n^{th} power of xy^{-1} is equal to the identity. This is the case because

$$\begin{aligned}(xy^{-1})^n &= x^n (y^{-1})^n \text{ (} A \text{ is abelian.)} \\ &= x^n (y^n)^{-1}\end{aligned}$$

and since x is an element of T , it must be that $x^n = 1$, so

$$= 1 \cdot (y^n)^{-1} = (y^n)^{-1}$$

and similarly, since y is an element of T , it must be that $y^n = 1$, so

$$= (1)^{-1} = 1.$$

So the n^{th} power of xy^{-1} is the identity, so $xy^{-1} \in T$. Thus, by the subgroup criterion, T is a subgroup of A . Whew, we're done!