Mathematics 546 Homework.

Recall that a map $\varphi\colon G_1 \to G_2$ is between groups is a ***homomorphism*** if and only if

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

If is also bijective (that is one to one and onto) then it is an ***isomorphism***. In that case the inverse map $\varphi^{-1}\colon G_2 \to G_1$ is also an isomorphism. If there is an isomorphism between the two groups G_1 and G_2, then they at ***isomorphic*** and we write $G_1 \cong G_2$.

We have proven the following a couple of times.

Proposition 1. *If $\varphi\colon G_1 \to G_2$ is an isomorphism, then for any $a \in G_1$ we have $o(\varphi(a)) = o(a)$.* $\square$

Therefore if G_1 has an element of some order n, but G_2 does not have any elements of order n, then G_1 and G_2 can not be isomorphic.

Problem 1. Use this idea to show that the groups $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not isomorphic to $\mathbb{Z}_9$. $\square$

Problem 2. Recall that the alternating groups A_n is the set of even elements in S_n and that it has size $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$. For example A_4 has order 12 and

$$\begin{aligned} A_4 = \{1,&(12)(34), (13)(24), (14)(23), \\ &(123), (132), (124), (142), (134), (143), (234), (243)\} \end{aligned}$$

The dihedral group D_6 also has 12 elements:

$$D_6 = \{1, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5b\}$$

where, as usual, $a^6 = b^2 = 1$ and $ba = a^{-1}b = a^5b$. Complete the following tables for elements of A_4 and D_6 showing their orders.

Element	order
1	1
(12)(34)	
(13)(24)	
(14)(23)	
(123)	
(132)	
(124)	
(142)	
(134)	
(143)	
(234)	
(243)	

Element	order
1	1
a	
a^2	
a^3	
a^4	
a^5	
b	
ab	
a^2b	
a^3b	
a^4b	
a^5b	

Problem 3. Use the previous problem to show A_4 and D_6 are not isomorphic. $\square$

In some of the problems that follow you will be ask to show that a function is an isomorphism, and in particular that it is bijective. The following is a basic fact that often makes this easier.

Proposition 2. *Let $\varphi\colon A \to B$ be a map between sets and assume there is a function $\psi\colon B \to A$ such that $\psi(\varphi(a)) = a$ for all $a \in A$ and $\varphi(\psi(b)) = b$ for all $b \in B$. Then φ is bijective and its inverse is $\varphi^{-1} = \psi$.*

Proof. We first show φ is surjective, that is onto. Let $b \in B$, then we need to find $a \in A$ with $\varphi(a) = b$. Then $a = \psi(b)$ works as then $\varphi(b) = \varphi(\psi(b)) = b$.

To see that φ is injective we need to show that if $\varphi(a_1) = \varphi(a_2)$, then $a_1 = a_2$. Starting with

$$\varphi(a_1) = \varphi(a_2)$$

we apply ψ to both sides and using that $\psi(\varphi(a)) = a$ for all $a \in A$ we get

$$a_1\psi(\varphi(a_1)) = \psi(\varphi(a_2)) = a_2$$

showing that φ is injective.

Thus φ is surjective and injective and therefore bijective. That $\psi = \varphi^{-1}$ is just the definition of the inverse φ^{-1}. □

Example 3. Here is an example of using this. Let $|G|$ be a group of order 17 and define $\varphi\colon G \to G$ by

$$\varphi(a) = a^3.$$

Show that φ is bijective. *Solution:* As $|G| = 17$ we know that $a^{17} = 1$ for all $a \in G$. Therefore $a^{18} = a^{17}a = a$ for all $a \in G$. This suggests defining $\varphi(a) = a^6$. Then

$$\begin{aligned}\varphi(\psi(a)) &= \varphi(a^6) = (a^6)^3 = a^{18} = a\\ \psi(\varphi(a)) &= \psi(a^3) = (a^3)^6 = a^{18} = a.\end{aligned}$$

Therefore by Proposition 2 φ is bijective. □

Problem 4. Let G be a group and $a \in G$. Define a map $\varphi_a\colon G \to G$ by

$$\varphi_a(x) = axa^{-1}.$$

Show that φ_a is an isomorphism of G with itself. *Hint:* There are two parts to this. First to show that φ_a is a homomorphism, that is $\varphi_a(xy) = \varphi_a(x)\varphi_a(y)$. The second part is to show that φ_a is bijective. Here using Proposition 2 can make life easier. Let $\psi = \varphi_{a^{-1}}$ (or more expliclity $\varphi_{a^{-1}}(x) = a^{-1}xa$) and show $\psi(\varphi_a(x)) = \varphi_a(\psi(x)) = x$ for all $x \in G$. □

We give a name to isomorphisms of a group with itself. An ***automorphism*** of a group G is an isomorphism $\varphi\colon G \to G$. So a restatement of the previous problem is that the map φ_a is a automorphism of G. The map φ_a is an ***inner automorphism***.

Problem 5. If $a, b \in G$ with G a group, and φ_a and φ_b defined as in Problem 4 show $\varphi_a \circ \varphi_b = \varphi_{ab}$. □

Problem 6. Let G be a finite Abelian group and k an integer relatively prime to $|G|$. Show the map $\varphi\colon G \to G$ given by $\varphi(a) = a^k$ is an automorphism of G. *Hint:* First show that φ is a homomorphism. Then you need to show φ is a bijection. As usual there are many ways to do this. One way to start is to let $n = |G|$. As k and n are relatively prime there are integers r and s with $rk + sn = 1$. Define $\psi\colon G \to G$ by $\psi(a) = a^r$ and show $\psi(\varphi(a)) = \varphi(\psi(a)) = a$ for all $a \in G$ and therefore $\psi = \varphi^{-1}$. A some point in showing this you will have to use that $a^n = 1$ for all $a \in G$. $\square$

Proposition 4. *Let $\varphi\colon G_1 \to G_2$ and $\psi\colon G_2 \to G_3$ be homomorphisms between groups. Then the composition $\psi \circ \varphi\colon G_1 \to G_3$ is also a homomorphism.*

Problem 7. Prove this. $\square$

The following form of the first homomorphism differs slightly from the version be gave in class.

Theorem 5. *Let $\varphi\colon G_1 \to G_2$ be a surjective (that is onto) homomorphism of groups and let*

$$K = \ker(\varphi) = \{x \in G_1 : \varphi(x) = e_2\}.$$

Then K is a normal subgroup of G_1 and

$$G_1/K \cong G_2.$$

(That is the quotient group G_1/K is isomorphic to G_2.)

Problem 8. Prove this theorem along the lines.

(a) We have shown elsewhere that K is a normal subgroup of G_1, and that G_1/K is a group with the product $(xK)(yK) = xyK$, so you can assume this for the rest of the proof.

(b) Define a map $\overline{\varphi}\colon G_1/K \to G_2$ by

$$\overline{\varphi}(xK) = \varphi(x).$$

Show this is well defined. That is for this definition to make sense we need that if $x_1K = x_2K$, then $\varphi(x_1) = \varphi(x_2)$, and this is what you should show.

(c) Show $\overline{\varphi}$ is a group homomorphism. That is show

$$\overline{\varphi}\big((xK)(yK)\big) = \overline{\varphi}(xK)\,\overline{\varphi}(yK).$$

(d) Now that we know $\overline{\varphi}$ is a homomorphism, we need to show it is a bijection. Start by showing surjective (i.e. onto. This is where you will use that φ is surjective).

(e) Finish the proof by showing $\overline{\varphi}$ is injective (i.e. one to one). Explicitly you need to show: if $\overline{\varphi}(xK) = \overline{\varphi}(yK)$, then $xK = yK$. $\square$

Definition 6. If $\varphi\colon G_1 \to G_2$ is a homomorphism between groups, then let

$$\operatorname{Image}(\varphi) = \varphi[G_1] = \{\varphi(x) : x \in G_1\}.$$

This is the ***image*** of G_1 by φ. $\square$

Proposition 7. *If* $\varphi\colon G_1 \to G_2$ *is homomorphism between groups, then* $\operatorname{Image}(\varphi)$ *is a subgroup of* G_2*.*

Problem 9*.* Prove this. $\square$

Here is the form of the first homomorphism theorem we gave in class.

Theorem 8. *Let* $\varphi\colon G_1 \to G_2$ *is homomorphism between groups. Then*

$$G/\ker(\varphi) \cong \operatorname{Image}(\varphi).$$

Problem 10*.* Prove this by letting $G_3 = \operatorname{Image}(\varphi)$ and noting that $\varphi\colon G_1 \to G_3 = \operatorname{Image}(\varphi)$ is surjective, so that we can just refer to Theorem 5 and not have to go though the whole proof again. $\square$

Problem 11*.* Let n be an integer with $2 \mid n$, $3 \mid n$, $5 \mid n$ (that is n is divisible be all three of the numbers 2, 3, and 5). Show $30 \mid n$ (that is n is divisible by 30.) $\square$

Problem 12*.* Show that as additive groups that

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{30}.$$

Hint: Define $\varphi\colon \mathbb{Z} \to \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ by

$$\varphi(k) = ([k]_2, [k]_3, [k]_5).$$

(a) Show φ is a group homomorphism. Note that since in this case the group operations are addition, this means showing $\varphi(k+\ell) = \varphi(k) + \varphi(\ell)$.

(b) Use Problem 11 to show

$$\ker(\varphi) = \{n : 30 \mid n\} = \{30q : q \in \mathbb{Z}\} = 30\mathbb{Z}.$$

and therefore

$$\mathbb{Z}/\ker(\varphi) = \mathbb{Z}/30\mathbb{Z} = \mathbb{Z}_{30}$$

(c) Therefore by Theorem 8 we have

$$\mathbb{Z}_{30} = \mathbb{Z}/\ker(\varphi) \cong \operatorname{Image}(\varphi).$$

(d) Finish the proof by noting $|\operatorname{Image}(\varphi)| = |\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5| = 30$ and so $\operatorname{Image}(\varphi)$ must be all of $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$. $\square$