Nathan Bickel
MATH 701: Section 001
Professor: Dr. Tsai
September 25, 2024

MATH 701 Homework 3

Let G and H be groups, and let $1_G, 1_H$ be the identities of G and H.

Problem 1.6.1 Let $\varphi : G \to H$ be a homomorphism.

(a) Prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$.

(b) Do part (a) for $n = -1$ and deduce that $\varphi(x^n) = \varphi(x)^n$.

(a) This follows quickly from induction. The base case is trivial. For the induction step, let $n \in \mathbb{N}$ and suppose that for all $n' < n$, $\varphi(x^{n'}) = \varphi(x)^{n'}$. Then we have

$$\varphi(x^n) = \varphi(x^{n-1}x) = \varphi(x)^{n-1}\varphi(x) = \varphi(x)^n$$

by the homomorphism property and induction hypothesis.

(b) Using the homomorphism property, we have

$$\varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(1_G) = 1_H$$

and

$$\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(1_G) = 1_H,$$

so the inverse of $\varphi(x)$ is $\varphi(x^{-1})$. Thus, $\varphi(x)^{-1} = \varphi(x^{-1})$. Let $n \in \mathbb{Z}$. If $n \geq 0$, then we have $\varphi(x^n) = \varphi(x)^n$ from part (a). Otherwise, $-n > 0$, and we have

$$\varphi(x^n) = \varphi\left(\left(x^{-1}\right)^{-n}\right) = \varphi(x^{-1})^{-n} = \left(\varphi(x)^{-1}\right)^{-n} = \varphi(x)^n.$$

Therefore, $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$. $\square$

Problem 1.6.2 If $\varphi : G \to H$ is an isomorphism, prove that $\left|\varphi(x)\right| = |x|$ 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?

Let $x \in G$ and $n := |x|$. Then we have

$$\varphi(x)^n = \varphi(x^n) = \varphi(1_G) = 1_H$$

by Problem 1.6.1, so $|\varphi(x)| \leq n$. Now let n' such that $\varphi(x)^{n'} = 1_H$. Then we have

$$\varphi(x^{n'}) = \varphi(x)^{n'} = 1_H = \varphi(1_G),$$

so since φ is an isomorphism and thus injective we have $x^{n'} = 1_G$. So we must have $n' \geq |x|$, and thus $|\varphi(x)| \geq |x|$. Therefore $|\varphi(x)| = |x|$.

It follows quickly that two isomorphic groups have the same number of elements of order n for all $n \in \mathbb{N}$: all the elements of order n in one group will have order n under the isomorphism in the other group, and visa versa.

The result is not true in general if φ is not injective, as this is used in the proof. An example where the order of $\varphi(x)$ is less than x is easy to construct.

Problem 1.6.3 If $\varphi : G \to H$ is an isomorphism, prove that G is abelian if and only if H is abelian. If $\varphi : G \to H$ is a homomorphism, what additional conditions on φ (if any) are sufficient to ensure that if G is abelian, then so is H?

($\Rightarrow$) Suppose G is abelian. Let $c, d \in H$, and let $a := \varphi^{-1}(c)$ and $b := \varphi^{-1}(d)$. Then we have

$$cd = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = dc.$$

($\Leftarrow$) Suppose H is abelian. Let $a, b \in G$. Then we have

$$\varphi(ab) = \varphi(a)\varphi(b) = \varphi(b)\varphi(a) = \varphi(ba),$$

so $ab = ba$ by the injectivity of φ.

It is sufficient for φ to be surjective: we can rewrite the proof of the forward direction to be such that a and b are elements of G such that $\varphi(a) = c$ and $\varphi(b) = d$, which are guaranteed to exist by surjectivity. $\square$

Problem 1.6.4 Prove that the multiplicative groups $\mathbb{R} \setminus \{0\}$ and $\mathbb{C} \setminus \{0\}$ are not isomorphic.

We have that $|i| = 4$ in $\mathbb{C}$, but there are no elements of order 4 in $\mathbb{R}$. So by Problem 1.6.1, no isomorphism can exist.

Problem 1.6.5 Prove that the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic.

Since $\mathbb{R}$ and $\mathbb{Q}$ are different cardinalities (by the Cantor diagonalization argument), there is no bijection between them. Therefore, no isomorphism can exist.

Problem 1.6.8 Prove that if $n \neq m$, S_n and S_m are not isomorphic.

Since the factorial function is injective, we have $|S_n| = n! \neq m! = |S_m|$, so the cardinalities are different. Therefore, no bijection and therefore no isomorphism can exist.

Problem 1.6.13 Let $\varphi : G \to H$ be a homomorphism. Prove that the image of φ, $\varphi(G)$, is a subgroup of H. Prove that if φ is injective then $G \cong \varphi(G)$.

Let $c, d \in \varphi(G)$ and let $a, b \in G$ such that $c = \varphi(a), d = \varphi(b)$. Then we have

$$cd^{-1} = \varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}),$$

which is in $\varphi(G)$ since $ab^{-1} \in G$. Since $1_H \in \varphi(G)$, then, $\varphi(G)$ is a subgroup of H.

Suppose φ is injective. Then define $\psi : G \to \varphi(G)$ by $\psi(g) = \varphi(g)$. Clearly, ψ is also an injective homomorphism, and it is surjective by definition. Thus, ψ is an isomorphism from G to $\varphi(G)$. $\square$

Problem 1.6.14 Let $\varphi : G \to H$ be a homomorphism. Define the kernel of φ to be $\{g \in G \mid \varphi(g) = 1_H\}$ (so the kernel is the set of elements in G which map to the identity of H, i.e., is the fiber over the identity of H). Prove that the kernel of φ is a subgroup of G. Prove that φ is injective if and only if the kernel of φ is the identity subgroup of G.

Let $a, b \in \ker(\varphi)$. Then we have

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = 1_H 1_H^{-1} = 1_H,$$

so $ab^{-1} \in \ker(\varphi)$. Therefore, $\ker(\varphi)$ is a subgroup of G (since it is non-empty). $\square$

($\Rightarrow$) Suppose φ is injective. Since we have that $\varphi(1_G) = 1_H$, any $a \in G$ such that $\varphi(a) = 1_H$ will satisfy $a = 1_G$ by injectivity. So $\ker(\varphi) = \{1_G\}$.

($\Leftarrow$) Suppose $\ker(\varphi) = \{1_G\}$. Let $a, b \in G$ such that $\varphi(a) = \varphi(b)$. Then we have $\varphi(a)\varphi(b)^{-1} = 1_H$, so $\varphi(ab^{-1}) = 1_H$ and thus $ab^{-1} \in \ker(\varphi)$. Thus we must have $ab^{-1} = 1_G$ (since 1_G is the only element in $\ker(\varphi)$), so $a = b$. Therefore, φ is injective. $\square$

Problem 1.6.18 Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

($\Rightarrow$) Suppose φ is a homomorphism. Let $a, b \in G$. Then we have

$$a(ab)b = a^2b^2 = \varphi(a)\varphi(b) = \varphi(ab) = (ab)^2 = a(ba)b$$

by the homomorphism property. Left-multiplying by a^{-1} and right-multiplying by b^{-1} then yields $ab = ba$.

($\Leftarrow$) Suppose G is abelian. Let $a, b \in G$. Then we have

$$\varphi(a)\varphi(b) = a^2b^2 = a(ab)b = a(ba)b = (ab)^2 = \varphi(ab)$$

by commutativity, so φ is a homomorphism. $\square$

Problem 1.6.20 Let $\text{Aut}(G)$ be the set of all isomorphisms from G onto G. Prove that $\text{Aut}(G)$ is a group under function composition (called the automorphism group of G and the elements of $\text{Aut}(G)$ are called automorphisms of G).

We prove the axioms:

- **Closure:** Let $\sigma, \tau \in \text{Aut}(G)$. We claim that $\sigma\tau$ is an automorphism of G. Let $a, b \in G$. Then we can use that σ and τ are both homomorphisms to write

$$\sigma\tau(ab) = \sigma(\tau(ab)) = \sigma(\tau(a)\tau(b)) = \sigma(\tau(a))\sigma(\tau(b)) = \sigma\tau(a)\sigma\tau(b),$$

  showing that $\sigma\tau$ is a homomorphism. Since σ and τ are both bijective, there exist inverses σ^{-1} and τ^{-1}. So $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$ exists, and thus $\sigma\tau$ is bijective. So $\sigma\tau$ is an automorphism of G.

- **Associativity:** Function composition is known to be associative.

- **Identity:** The identity function id_G is clearly in $\text{Aut}(G)$.

- **Inverses:** Any $\sigma \in \text{Aut}(G)$ has an inverse σ^{-1} since it is bijective, and since σ^{-1} is also an automorphism, it is in $\text{Aut}(G)$.

Therefore, $\mathrm{Aut}(G)$ is a group under function composition. $\square$

Problem 1.6.23 Let G be a finite group which possesses an automorphism σ such that $\sigma(g) = g$ if and only if $g = 1$. If σ^2 is the identity map from G to G, prove that G is abelian (such an automorphism σ is called fixed point free of order 2).

Define $f : G \to G$ by $f(x) = x^{-1}\sigma(x)$ for all $x \in G$. We claim that f is injective. To see this, let $x, y \in G$ such that $f(x) = f(y)$. Then we have

$$\begin{aligned}
& f(x) = f(y) \\
\implies & x^{-1}\sigma(x) = y^{-1}\sigma(y) \\
\implies & \sigma(x)\sigma(y)^{-1} = xy^{-1} && \text{(multiplying by inverses)} \\
\implies & \sigma(xy^{-1}) = xy^{-1} && \text{(homomorphism property)} \\
\implies & xy^{-1} = 1 && \text{(property of } \sigma\text{)} \\
\implies & x = y.
\end{aligned}$$

So f is injective. Since G is finite, it follows that f is a bijection since the domain equals the codomain.

We now show that G is abelian. Let $a, b \in G$, and set $\alpha := f^{-1}(a), \beta := f^{-1}(b)$. Then, we have

$$\begin{aligned}
ab\sigma(ba) &= f(\alpha)f(\beta)\sigma\left(f(\beta)f(\alpha)\right) \\
&= \alpha^{-1}\sigma(\alpha)\beta^{-1}\sigma(\beta)\sigma\left(\beta^{-1}\sigma(\beta)\alpha^{-1}\sigma(\alpha)\right) \\
&= \alpha^{-1}\sigma(\alpha)\beta^{-1}\sigma(\beta)\sigma(\beta^{-1})\sigma(\sigma(\beta))\sigma(\alpha^{-1})\sigma(\sigma(\alpha)) && \text{(homomorphism property)} \\
&= \alpha^{-1}\sigma(\alpha)\beta^{-1}\sigma(\beta)\sigma(\beta)^{-1}\beta\sigma(\alpha)^{-1}\alpha && \text{(using } \sigma^2 = id_G\text{)} \\
&= 1, && \text{(repeated cancellation of inverses)}
\end{aligned}$$

and a similar calculation shows that $\sigma(ba)ab = 1$. So we have

$$\begin{aligned}
& ab\sigma(ba) = \sigma(ba)ba \\
\implies & ab(ba)^{-1} = \sigma(ab)^{-1}\sigma(ab) \\
\implies & ab(ba)^{-1} = 1 \\
\implies & ab = ba.
\end{aligned}$$

Therefore, G is abelian. $\square$