MAT301 Groups and Symmetry

Assignment 4

Solutions

1. (a) Let $\phi : G \to H$ be a homomorphism. Let $g \in G$. Show that $\phi(\langle g \rangle) = \langle \phi(g) \rangle$ (i.e that the image of the subgroup generated by g under ϕ is the subgroup generated by $\phi(g)$).

(b) Conclude that the image of a cyclic group under a homomophism is cyclic (i.e. that if G is cyclic and $\phi : G \to H$ is a homomorphism, then $\phi(G)$ is cyclic).

(c) Let G and H be isomorphic groups. Show that G is cyclic if and only if H is cyclic.

Solution: (a) This follows from that for every n, we have $\phi(g^n) = \phi(g)^n$. Indeed, given any $g' \in \langle g \rangle$, we have $g' = g^n$ for some n, so that $\phi(g') = \phi(g^n) = \phi(g)^n \in \langle \phi(g) \rangle$, hence $\phi(\langle g \rangle) \subset \langle \phi(g) \rangle$. On the other hand, given $h \in \langle \phi(g) \rangle$, we have $h = \phi(g)^n$ for some n, so that $h = \phi(g^n) \in \phi(\langle g \rangle)$. Thus $\langle \phi(g) \rangle \subset \phi(\langle g \rangle)$.

(b) Let G be cyclic and $\phi : G \to H$ a homomorphism. If G is generated by g, by Part (a), $\mathrm{Im}(\phi)$ is generated by $\phi(g)$ and is cyclic.

(c) Let $\phi : G \to H$ be an isomorphism. In particular, ϕ is a surjective homomorphism, so that (by (b)) if G is cyclic, then so is $\mathrm{Im}(\phi) = H$.

2. (a) For any two groups G and H, we denote the set of all homomorphisms $G \to H$ by $\mathrm{Hom}(G, H)$. Show that for any group H, there is a bijective function

$$\mathrm{Hom}(\mathbb{Z}, H) \to H.$$

(Suggestion: Define $F : \mathrm{Hom}(\mathbb{Z}, H) \to H$ by $F(\phi) = \phi(1)$. Thus F sends a homomorphism $\phi : \mathbb{Z} \to H$ simply to $\phi(1) \in H$. Show that F is a bijection. Injectivity of F is the statement that if ϕ and ψ are homomorphisms $\mathbb{Z} \to H$ and $\phi(1) = \psi(1)$, then $\phi = \psi$ (i.e., that a homomorphism $\mathbb{Z} \to H$ is *determined* by its value at 1.) Surjectivity of F is the statement that for any $h \in H$, there is a homomorphism $\phi : \mathbb{Z} \to H$ such that $\phi(1) = h$.)

(b) List all homomorphisms $\mathbb{Z} \to S_3$.

Solution: (a) Let F be the function defined in the suggestion. We show that F is bijective.

- Injectivity: Let $\phi, \psi \in \mathrm{Hom}(\mathbb{Z}, H)$ (so ϕ and ψ are homomorphisms $\mathbb{Z} \to H$). Suppose $F(\phi) = F(\psi)$, which means $\phi(1) = \psi(1)$. Then for every integer n,

  $$\phi(n) = \phi(1)^n = \psi(1)^n = \psi(n),$$

  where in the first (resp. last) equality we used the fact that ϕ (resp. ψ) is a homomorphism, and in the middle equality we used the assumption that $\phi(1) = \psi(1)$. Thus $\phi = \psi$.
- Surjectivity:Let $h \in H$. Define $\phi : \mathbb{Z} \to H$ by $\phi(n) = h^n$. Then ϕ is a homomorphism, as

  $$\phi(m + n) = h^{m+n} = h^m h^n = \phi(m)\phi(n).$$

We have $F(\phi) = \phi(1) = h$.

(b) For each $\sigma \in S_3$, define $\phi_\sigma : \mathbb{Z} \to S_3$ by $\phi_\sigma(n) = \sigma^n$. The ϕ_σ are all the homomorphisms $\mathbb{Z} \to S_3$. More explicitly, homomorphisms $\mathbb{Z} \to S_3$ are the followings: 1) $n \mapsto e$ (the trivial homomorphism), 2) $n \mapsto (12)^n$, 3) $n \mapsto (23)^n$, 4) $n \mapsto (13)^n$, 5) $n \mapsto (123)^n$, and 6) $n \mapsto (132)^n$.

3. Let G and H be finite groups such that $|G|$ and $|H|$ are relatively prime. Show that the only homomorphism $G \to H$ is the trivial map. In other words, show that if $\phi : G \to H$ is a homomorphism, then $\phi(g) = e$ for every $g \in G$. (Suggestion: Use Lagrange's theorem and the fact that $|\phi(g)| \mid |g|$.)

Solution: Let $\phi : G \to H$ be a homomorphism. Let $g \in G$. We need to show that $\phi(g) = e$. Since ϕ is a homomorphism and g has finite order, we have $|\phi(g)| \mid |g|$ (for $\phi(g)^{|g|} = \phi(g^{|g|}) = \phi(e) = e$). By Lagrange's theorem (applied to the group G) we have $|g| \mid |G|$, so that $|\phi(g)| \mid |G|$. On the other hand, Lagrange's theorem (this time applied to the group H) also implies $|\phi(g)| \mid |H|$. Since $|G|$ and $|H|$ are relatively prime, it follows that $|\phi(g)| = 1$, i.e. $\phi(g) = e$.

4. Show that the only homomorphism $\mathbb{Q} \to \mathbb{Q}^\times$ is the trivial map.

Solution: Let $\phi : \mathbb{Q} \to \mathbb{Q}^\times$ be a homomorphism. Suppose $\phi(a) \neq 1$ for some $a \in \mathbb{Q}$. Let $b = \phi(a)$. Since $b \in \mathbb{Q} - \{0, 1\}$, there exists a positive integer n such that the equation $x^n = b$ does not have a rational solution (let us take this for granted - to prove it one uses unique factorization of integers as products of prime numbers). But we have

$$b = \phi(a) = \phi(n \cdot \frac{a}{n}) \overset{\text{why}}{=} \phi(\frac{a}{n})^n,$$

which is a contradiction as $x = \phi(\frac{a}{n})$ is in $\mathbb{Q}$ and satisfies $x^n = b$.

5. (a) Let G be a group. We say a subgroup $K \leq G$ is *normal* if for every $k \in K$ and $g \in G$, the element gkg^{-1} is in K. Let $\phi : G \to H$ be a homomorphism. Show that the subgroup $\ker(\phi)$ of G is a normal subgroup. (You don't have to rewrite the proof of the fact that the kernel is a subgroup; just verify normality.)

(b) Is there a homomorphism with domain S_{10} whose kernel is $\{e, (12)\}$? (Justify your answer.)

Solution: (a) Let $k \in \ker(\phi)$ and $g \in G$. We have

$$\phi(gkg^{-1}) \overset{\text{why}}{=} \phi(g)\phi(k)\phi(g^{-1}) \overset{\text{why}}{=} \phi(g)e_H\phi(g^{-1}) \overset{\text{why}}{=} \phi(g)(\phi(g))^{-1} = e_H.$$

Thus $gkg^{-1} \in \ker(\phi)$.

(b) By (a), it is enough to show that the subgroup $K := \{e, (12)\}$ of S_{10} is not normal. Take $g = (13)$, $k = (12) \in K$. We have

$$gkg^{-1} = (13)(12)(13)^{-1} = (13)(12)(13) = (23) \notin K,$$

showing that K is not a normal subgroup of S_{10}.

6. Determine which of the following groups are isomorphic: $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{R}^\times$, $\mathbb{R}_{>0}$ (under multiplication), $\mathbb{C}^\times$, S_3, μ_6, $U(9)$, D_4, $\mathbb{Z}/8$, $U(16)$.

You may take the following fact for granted: two cyclic groups of the same order are isomorphic. (We will prove this in the next lecture.)

Solution: Note that $\mathbb{Z}$ and $\mathbb{Q}$ are infinite and countable, while $\mathbb{R}$, $\mathbb{R}^\times$, $\mathbb{R}_{>0}$, $\mathbb{C}^\times$ are uncountable, S_3, μ_6, $U(9)$ have order 6, and D_4, $\mathbb{Z}/8$, $U(16)$ have order 8. It follows that if two groups on our list are isomorphic to each other, they both belong to one of the following families:

(i) $\mathbb{Z}$ and $\mathbb{Q}$
(ii) $\mathbb{R}$, $\mathbb{R}^\times$, $\mathbb{R}_{>0}$, and $\mathbb{C}^\times$
(iii) S_3, μ_6 and $U(9)$
(iv) D_4, $\mathbb{Z}/8$, and $U(16)$.

(i) $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic to one another since $\mathbb{Z}$ is cyclic but $\mathbb{Q}$ is not. (In fact, you can prove that there is no nontrivial homomorphism $\mathbb{Q} \to \mathbb{Z}$.)

(ii) $\mathbb{R}$ and $\mathbb{R}_{>0}$ are indeed isomorphic; an isomorphism $\mathbb{R} \to \mathbb{R}_{>0}$ is given by the exponential map $x \mapsto e^x$. These are the only groups on the list that isomorphic to one another: $\mathbb{C}^\times$ has infinitely many elements of finite order (all complex roots of unity), $\mathbb{R}^\times$ has two such elements (± 1), whereas $\mathbb{R}$ (and $\mathbb{R}_{>0}$) only have one element of finite order.

(iii) μ_6 are $U(9)$ are cyclic of order 6, hence isomorphic. The group S_3 on the other hand is not abelian is not isomorphic to either of μ_6 or $U(9)$ (which are abelian).

(iv) D_4 is not abelian but $\mathbb{Z}/8$ and $U(16)$ are, so D_3 is not isomorphic to any of the latter two groups. Te group $\mathbb{Z}/8$ is cyclic and $U(16)$ is not, so $\mathbb{Z}/8$ and $U(16)$ are not isomorphic.

Thus to summarize, the only isomorphic groups among the given groups are $\mathbb{R} \simeq \mathbb{R}_{>0}$ and $\mu_6 \simeq U(9)$.