MATH 6121: selected solutions

Written and formatted by John M. Campbell
jmaxwellcampbell@gmail.com

Exercise 1: Prove that if $\phi\colon G \to H$ is a homomorphism, then $\text{im}(\phi) \leq H$ with respect to $\circ_H$, where $\text{im}(\phi) = \{\phi(g) : g \in G\}$.

Proof: Given a subset S of the underlying set of a group T, to prove that S forms a subgroup of T, it suffices to prove that S is closed under the underlying binary operation of T and that S is closed under inverses with respect to this operation. This property concerning subgroups is sometimes referred to as the **Two-Step Subgroup Test** (see Joseph A. Gallian's *Contemporary Abstract Algebra*).

So, let g_1 and g_2 be arbitrary elements in G, so that $\phi(g_1)$ and $\phi(g_2)$ are arbitrary elements in $\text{im}(\phi)$. Since $\phi\colon G \to H$ is a homomorphism, we have that

$$\phi(g_1) \circ_H \phi(g_2) = \phi(g_1 \circ_G g_2) \in \text{im}(\phi),$$

thus proving that $\text{im}(\phi)$ is closed with respect to $\circ_H$. Similarly, we have that

$$(\phi(g))^{-1} = \phi(g^{-1}) \in \text{im}(\phi)$$

for $g \in G$, since

$$(\phi(g))^{-1}\phi(g) = e_H = \phi(e_G) = \phi(g^{-1}g) = \phi(g^{-1})\phi(g)$$

since a group homomorphism must map a group identity element to another group identity element, since $\phi(e_G g) = \phi(g) = \phi(e_G)\phi(g)$, and thus $\phi(e_G) = e_H$ from the equality $\phi(g) = \phi(e_G)\phi(g)$.

Exercise 2: Prove that $\ker(\phi) \trianglelefteq G$, where $\ker(\phi) = \{g \in G \mid \phi(g) = e_H\}$.

Proof: We begin by proving that $\ker(\phi) \leq G$, using the Two-Step Subgroup Test described above.

Let $g_1, g_2 \in G$ be such that $\phi(g_1) = e_H$ and $\phi(g_2) = e_H$, so that g_1 and g_2 are arbitrary elements in the kernel $\ker(\phi)$ of the group homomorphism $\phi\colon G \to H$. We thus have that

$$\phi(g_1) \circ \phi(g_2) = \phi(g_1 \circ g_2) = e_H \circ e_H = e_H,$$

thus proving that $g_1 \circ g_2 \in \ker(\phi)$. Similarly, since for $g \in G$ we have that $(\phi(g))^{-1} = \phi(g^{-1})$ as discussed above, we have that

$$(\phi(g))^{-1} = e_H^{-1} = e_H$$

if $g \in \ker(\phi)$ and thus $\phi(g^{-1}) = e_H$ if $g \in \ker(\phi)$, thus proving that $\ker(\phi) \leq G$.

Now, let $k \in \ker(\phi)$, and let $i \in G$. It remains to prove that: $iki^{-1} \in \ker(\phi)$. Equivalently, it remains to prove that $\phi(iki^{-1}) = e_H$. Using the fact that $k \in \ker(\phi)$, we have that

$$\phi(iki^{-1}) = \phi(i)\phi(k)\phi(i^{-1}) = \phi(i)\phi(i^{-1}) = \phi(i \circ i^{-1}) = \phi(e_G) = e_H,$$

thus proving that $\ker(\phi) \trianglelefteq G$.

Exercise 3: Given a group G and a group action $\bullet \colon G \times G \to G$ given by G acting on itself canonically, prove that the mapping which sends $g \in G$ to the permutation in S_G given by the mapping $h \mapsto g \bullet h$ is an isomorphism.

Proof: Let ψ denote the mapping which maps $g \in G$ to the permutation in S_G given by the mapping $h \mapsto g \bullet h$, letting the codomain of ψ be equal to $\mathrm{im}(\psi)$.

First, we begin by proving that ψ is well-defined in the sense that for $g \in G$, $\psi(g)$ is indeed an element in the codomain of ψ. For $g \in G$, let σ_g denote the mapping $\sigma_g \colon G \to G$ whereby

$$\sigma_g(h) = g \bullet h = g \circ h \in G$$

for all $h \in G$. The mapping σ_g must be injective, since

$$\sigma_g(h_1) = \sigma_g(h_2) \Longrightarrow gh_1 = gh_2 \Longrightarrow h_1 = h_2,$$

and the mapping $\sigma_g \colon G \to G$ must be surjective, since for $k \in G$, we have that: $\sigma_g(g^{-1}k) = g \circ g^{-1} \circ k = k \in G$, thus proving that $\sigma_g \in S_G$, and thus proving that σ_g is in the codomain of ψ.

Now let $g_1, g_2 \in G$, and let $\sigma_{g_1} \colon G \to G$ and $\sigma_{g_2} \colon G \to G$ be such that $\sigma_{g_1}(h) = g_1 h \in G$ and $\sigma_{g_2}(h) = g_2 h \in G$ for all $h \in G$. Suppose that $\psi(g_1) = \psi(g_2)$. That is, $\sigma_{g_1} = \sigma_{g_2}$. That is, $g_1 h = g_2 h$ for all $h \in G$. Letting

$h = e$, we thus have that $\psi(g_1) = \psi(g_2) \implies g_1 = g_2$, thus proving that ψ is injective.

Since we constructed ψ so that the codomain of ψ is equal to the image of ψ, we have that ψ is surjective by definition. Since ψ is bijective, it remains to prove that ψ is a group homomorphism.

Again let $g_1, g_2 \in G$. We thus have that $\psi(g_1 g_2)$ is the mapping $\sigma_{g_1 g_2} \colon G \to G$ which maps h to $g_1 g_2 h$. But it is clear that the composition $\psi(g_1) \circ \psi(g_2)$ maps h to $g_1(g_2 h) = g_1 g_2 h$, thus proving that ψ is an isomorphism.

Exercise 4: For all $g_1, g_2 \in G$, show that either $g_1 H = g_2 H$ or $g_1 H \cap g_2 H = \varnothing$.

Proof: Let $g_1, g_2 \in G$. Our strategy is to show that if $g_1 H \cap g_2 H$ is nonempty, then $g_1 H = g_2 H$. We remark that we are using the logical equivalence whereby $(\neg p) \to q \equiv q \vee p$.

Suppose that $g_1 H \cap g_2 H$ is nonempty. Note that we are letting $H \leq G$. So there exists an element in the following intersection:

$$\{g_1 h : h \in H\} \cap \{g_2 h : h \in H\}.$$

We thus have that there exist elements h_1 and h_2 in H such that

$$g_1 h_1 = g_2 h_2 \in g_1 H \cap g_2 H.$$

Therefore,

$$g_1 h_1 h_2^{-1} = g_2.$$

Writing $h_3 = h_1 h_2^{-1} \in H$, we thus have that $g_1 h_3 = g_2$. We thus have that the left coset $g_2 H$ is equal to $\{g_1 h_3 h : h \in H\}$. But since the mapping from H to H which maps $h \in H$ to $h_3 h$ is bijective (see previous exercise), we have that

$$g_2 H = \{g_1 h_3 h : h \in H\} = \{h_1 i : i \in H\} = g_1 H$$

as desired.

Exercise 5: Show that the canonical mapping $\phi_g \colon H \to gH$ is a bijection, so that, as a consequence, we have that $|gH| = |H|$. Another consequence of this result is that $|H|$ divides $|G|$ (**Lagrange's theorem**).

Let $H \leq G$, and let $g \in G$, and let $\phi_g \colon H \to gH$ be such that $\phi_g(h) = gh \in gH$ for all $h \in H$. We have that

$$\phi_g(h_1) = \phi_g(h_2) \implies gh_1 = gh_2 \implies h_1 = h_2,$$

thus proving the injectivity of ϕ_g. Similarly, it is clear that ϕ_g is surjective, since for $gh \in gH$ we have that $\phi_g(h) = gh$. We thus have that $|gH| = |H|$ as desired.

We now use this result to prove Lagrange's theorem. From our results from **Exercise 4**, we have that two cosets g_1H and g_2H are either disjoint or equal. Therefore, since $g \in gH$ for all $g \in G$, we have that G may be written as a disjoint union of cosets, say

$$G = g_1H \cup g_2H \cup \cdots \cup g_nH$$

where $n \in \mathbb{N}$. But since $|gH| = |H|$ for $g \in G$, we have that $|G| = n|H|$, thus proving Lagrange's theorem.

Exercise 6: For $g \in G$, let $\text{order}(g)$ denote the smallest $n \in \mathbb{N}$ such that $g^n = e$. Prove that $\text{order}(g)$ divides $|G|$.

Proof: It is easily seen that the set

$$\{1, g, g^2, \ldots, g^{\text{order}(g)-1}\}$$

forms a cyclic subgroup of G. By Lagrange's theorem, proven above, we have that the order of this cyclic subgroup divides $|G|$, and we thus have that $\text{order}(g)$ divides $|G|$ as desired.

Exercise 7: Prove that $\text{Stab}(x)$ is a subgroup of G.

Proof: We again make use of the Two-Step Subgroup Test described above.

Let $g_1, g_2 \in G$ be such that $g_1 \bullet x = x$ and $g_2 \bullet x = x$, so that g_1 and g_2 are arbitrary elements in $\text{Stab}(x)$. Now consider the following expression: $(g_1g_2) \bullet x$. By definition of a group action, we have that

$$(g_1g_2) \bullet x = g_1 \bullet (g_2 \bullet x) = g_1 \bullet x = x,$$

thus proving that $\text{Stab}(x)$ is closed under the underlying binary operation of G. Letting $g \in G$ be such that $g \bullet x = x$, since $(g^{-1}g) \bullet x = e \bullet x = x$ by definition of a group action, we have that $g^{-1} \bullet (g \bullet x) = x$, thus proving that $g^{-1} \bullet x = x$ as desired, with $\mathrm{Stab}(x) \leq G$.

Exercise 8: Prove that a G-set X is a disjoint union of orbits.

Proof: Let x be a G-set, and let $\bullet\colon G \times X \to X$ denote a group action. Let $x, y \in X$, so that $\mathrm{Orbit}(x)$ and $\mathrm{Orbit}(y)$ are arbitrary orbits. Suppose that $\mathrm{Orbit}(x) \cap \mathrm{Orbit}(y) \neq \varnothing$. Let

$$g_1 \bullet x = g_2 \bullet y \in X$$

denote an element in the nonempty intersection $\mathrm{Orbit}(x) \cap \mathrm{Orbit}(y)$. We thus have that

$$(g_2^{-1} g_1) \bullet x = y.$$

Therefore,

$$\mathrm{Orbit}(y) = \{g \bullet (g_2^{-1} g_1 \bullet x) \mid g \in G\}.$$

Equivalently,

$$\mathrm{Orbit}(y) = \{g(g_2^{-1} g_1) \bullet x \mid g \in G\}.$$

Since the mapping whereby $g \mapsto g(g_2^{-1} g_1)$ is a permutation of G (see **Exercise 3**), we thus have that

$$\mathrm{Orbit}(y) = \{h \bullet x \mid h \in G\},$$

thus proving that two orbits are either equal or disjoint. Since $x \in \mathrm{Orbit}(x)$ for $x \in X$, we thus have that X may be written as a disjoint union of orbits.

Exercise 9: Show that the map

$$\phi_x\colon \mathrm{Orbit}(x) \to G/\mathrm{Stab}(x)$$

given by the mapping

$$g \bullet x \mapsto g\mathrm{Stab}(x) \in G/\mathrm{Stab}(x)$$

is a well-defined, bijective G-set homomorphism.

Proof: Suppose that $g_1 \bullet x = g_2 \bullet x$. Equivalently, $g_2^{-1} g_1 \bullet x = x$. Therefore, $g_2^{-1} g_1 \in \mathrm{Stab}(x)$, so $g_1 \in g_2\mathrm{Stab}(x)$, so $g_1\mathrm{Stab}(x) = g_2\mathrm{Stab}(x)$ (see **Exercise 4**). We thus have the mapping ϕ_x is well-defined in the sense that $g_1 \bullet x = g_2 \bullet x$ implies that $\phi_x(g_1 \bullet x) = \phi_x(g_2 \bullet x)$.

Letting $g_1, g_2 \in G$ so that $g_1 \bullet x$ and $g_2 \bullet x$ are arbitrary elements in the domain of ϕ_x, we have that

$$\phi_x(g_1 \bullet x) = \phi_x(g_2 \bullet x) \Longrightarrow g_1\mathrm{Stab}(x) = g_2\mathrm{Stab}(x).$$

We thus have that there exist elements $g_3, g_4 \in \mathrm{Stab}(x)$ such that

$$g_1g_3 = g_2g_4.$$

We thus have that

$$(g_1g_3) \bullet x = (g_2g_4) \bullet x,$$

which implies that

$$g_1 \bullet x = g_2 \bullet x,$$

thus proving the injectivity of ϕ_x. It is obvious that ϕ_x is surjective, since given a coset $g\mathrm{Stab}(x)$ in the codomain of ϕ_x, we have that $\phi_x(g) = g\mathrm{Stab}(x)$.

Since

$$\phi_x((hg) \bullet x) = (hg)\mathrm{Stab}(x) = h(g\mathrm{Stab}(x)) = h\phi_x(g \bullet x),$$

we have that ϕ_x is a G-set homomorphism.

Exercise 10: Prove that if $H \trianglelefteq G$, then G/H is a group where $\circ_{G/H}$ is defined as $g_1H \circ_{G/H} g_2H = g_1g_2H$.

Assume that $H \trianglelefteq G$. We begin by showing that the operation $\circ_{G/H} = \circ$ is *well-defined* in the sense that the expression $g_1H \circ_{G/H} g_2H$ does not depend on the coset representatives of the cosets g_1H and g_2H. So, suppose that $g_1H = g_3H$ and $g_2H = g_4H$, letting $g_1, g_2, g_3, g_4 \in G$. To prove that the operation $\circ_{G/H}$ is well-defined, it thus remains to prove that:

$$g_1g_2H = g_3g_4H.$$

Since $g_1H = g_3H$, let $g_3 = g_1h_1$, where $h_1 \in H$. Similarly, since $g_2H = g_4H$, let $g_4 = g_2h_2$, with $h_2 \in H$. So, it remains to prove that

$$g_1g_2H = g_1h_1g_2h_2H.$$

But since $H \trianglelefteq G$, we have that $gH = Hg$ for all $g \in G$. Since $h_1g_2 \in Hg_2 = g_2H$, let $h_1g_2 = g_2h_3$, where $h_3 \in H$. We thus have that

$$g_1h_1g_2h_2H = g_1g_2h_3h_2H.$$

But it is clear that

$$g_1 g_2 h_3 h_2 H = g_1 g_2 H$$

since the mapping $h \mapsto h_3 h_2 h$ is a bijection on H. We thus have that

$$g_3 g_4 H = g_1 g_2 H$$

as desired, thus proving that $\circ_{G/H}$ is well-defined.

Since $\circ_{G/H}$ maps elements in $(G/H) \times (G/H)$ to G/H, we have that G/H is a binary operation on G/H. So we have thus far shown that $\circ_{G/H}$ is a well-defined binary operation on G/H.

The binary operation $\circ_{G/H} = \circ$ inherits the associativity of the underlying binary operation of G in a natural way:

$$\begin{aligned} g_1 H \circ (g_2 H \circ g_3 H) &= g_1 H \circ ((g_2 g_3) H) \\ &= g_1 (g_2 g_3) H \\ &= (g_1 g_2) g_3 H \\ &= (g_1 g_2) H \circ g_3 H \\ &= (g_1 H \circ g_2 H) \circ g_3 H. \end{aligned}$$

We have thus far shown that $\circ_{G/H}$ is a well-defined associative binary operation on G/H.

Letting $g \in G$ be arbitrary, and letting $e = e_G$ denote the identity element in G, we have that:

$$\begin{aligned} (eH)(gH) &= (eg)H \\ &= eH \\ &= (ge)H \\ &= (gH)(eH). \end{aligned}$$

Again letting $g \in G$ be arbitrary, we have that:

$$\begin{aligned} (gH)(g^{-1}H) &= (g \cdot g^{-1})H \\ &= eH \\ &= (g^{-1}g)H \\ &= (g^{-1}H)(gH). \end{aligned}$$

We thus have that if $H \trianglelefteq G$, then G/H forms a group under the operation $\circ_{G/H}$ given above.

Exercise 11: Show that the mapping $\phi\colon G \to G/H$ is a group homomorphism, where $g \mapsto gH$ and $\ker(\phi) = H$.

Since $\ker(\phi) \trianglelefteq G$ as shown above, from our results given in the previous exercise, we have that G/H is a group with respect to the binary operation $\circ_{G/H}$.

Now let $g_1, g_2 \in G$. We thus have that

$$\phi(g_1 g_2) = (g_1 g_2)H = (g_1 H) \circ_{G/H} (g_2 H) = \phi(g_1) \circ_{G/H} \phi(g_2)$$

by definition of the well-defined group operation $\circ_{G/H}$.