Problem Set 3

Due Wednesday, September 17

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. You cannot use any resources besides me, your classmates, and our course notes.

I will post the .tex code for these problems for you to use if you wish to type your homework. If you prefer not to type, please *write neatly.* As a matter of good proof writing style, please use complete sentences and correct grammar. You may use any result stated or proven in class or in a homework problem, provided you reference it appropriately by either stating the result or stating its name (e.g. the definition of ring or Lagrange's Theorem). Please do not refer to theorems by their number in the course notes, as that can change.

Problem 1. For groups G and H, the group $G \times H$, known as the **product of G and H**, refers to the set

$$G \times H := \{(g, h) \mid g \in G, h \in H\}$$

equipped with the multiplication rule

$$(g_1, h_1) \cdot (g_2, h_2) := (g_1 \cdot_G g_2, h_1 \cdot_H h_2).$$

You may take it as a known fact that the product of two groups is also a group.

(1.1) Let G and H be groups, and consider elements $g \in G$ and $h \in H$, and the corresponding element $(g, h) \in G \times H$. Show that

$$\operatorname{ord}((g,h)) = \begin{cases} \operatorname{lcm}(\operatorname{ord}(g), \operatorname{ord}(h)) & \text{if } \operatorname{ord}(g), \operatorname{ord}(h) < \infty \\ \infty & \text{if } \operatorname{ord}(g) = \infty \text{ or } \operatorname{ord}(h) = \infty. \end{cases}$$

Proof. First suppose that $|g|$ and $|h|$ are both finite. Let $|g| = a$ and $|h| = b$, and let $\ell = \operatorname{lcm}(|g|, |h|)$. Since ℓ is a multiple of both a and b, we can write $\ell = ac$ and $\ell = bd$. Then

$$(g, h)^\ell = (g^{ac}, h^{bd}) = ((g^a)^c, (h^b)^d) = (e_G, e_H) = e_{G \times H}.$$

Thus $|(g, h)| \leqslant \ell$. Moreover, let $n := |(g, h)|$. Then $(g^n, h^n) = (g, h)^n = e$, so in particular $g^n = e$ and $h^b = e$. By a previous homework problem, we conclude that $|g|$ and $|h|$ both divide n, and thus n must be a multiple of $\operatorname{lcm}(|g|, |h|)$. In particular, $n \geqslant \operatorname{lcm}(|g|, |h|)$. We showed that $|(g, h)| \leqslant \operatorname{lcm}(|g|, |h|)$ and $\operatorname{lcm}(|g|, |h|) \geqslant |(g, h)|$, so we must have $\operatorname{lcm}(|g|, |h|) = |(g, h)|$.

For the other case, we show the contrapositive. Suppose that $(g, h) \in G \times H$ has finite order n. Then

$$(g^n, h^n) = (g, h)^n = (e_G, e_H),$$

so in particular $g^n = e$ and $h^n = e$. We conclude that g and h both have finite order. □

(1.2) For each of the following pairs of groups, show that the two groups are not isomorphic.

- $(\mathbb{C}, +)$ and $(\mathbb{Q}, +)$.

Proof. These groups are not isomorphic since $\mathbb{C}$ and $\mathbb{Q}$ have different cardinalities, and any isomorphism is in particular a bijection of sets. □

- $(\mathbb{R} \setminus \{0\}, \cdot)$ and $(\mathbb{R}, +)$.

  Proof. They are not isomorphic since $(\mathbb{R} \setminus \{0\}, \cdot)$ has one element of order 2, namely -1, while every element of $(\mathbb{R}, +)$ has infinite order. □

- $\mathbb{Z}/2 \times \mathbb{Z}/2$ and $\mathbb{Z}/4$.

  Proof. They are not isomorphic since $\mathbb{Z}/4$ has an element, $[1]$, of order 4 and $\mathbb{Z}/2 \times \mathbb{Z}/2$ has no such elements. □

- $Q_8 \times \mathbb{Z}/3$ and S_4.

  Proof. Since $|-1| = 2$ and $|[1]_3| = 3$, the element $(-1, [1])$ in $Q_8 \times \mathbb{Z}/3$ has order $\operatorname{lcm}(2, 3) = 6$. We claim that S_4 has no elements of order 6. However, S_4 has no elements of order 6, as we showed in the previous homework. □

Problem 2. Let

$$G = \prod_{i \in \mathbb{N}} \mathbb{Z} = \{(n_i)_{i \geqslant 0} \mid n_i \in \mathbb{Z}\}$$

be the group whose elements are sequences of integers, equipped with the operation given by componentwise addition. Let $H = (\mathbb{Z}, +)$. Show[1] that $G \times H \cong G$.

Proof. Consider the map that prepends an integer to a sequence of integers, more formally

$$f \colon G \times H \longrightarrow G$$

$$f((z_i)_{i \in \mathbb{N}}, h) = (h, z_0, z_1, z_2, \ldots).$$

We claim that this a group homomorphism. Indeed:

$$\begin{aligned} f((z_i)_{i \in \mathbb{N}}, a) + f((w_i)_{i \in \mathbb{N}}, b) &= (a, z_0, z_1, \ldots) + (b, w_0, w_1, \ldots) && \text{by definition of } f \\ &= (a + b, z_0 + w_0, z_1 + w_1, \ldots) && \text{by definition of } G \times H \\ &= f((z_i + w_i)_i, a + b) && \text{by definition of } f \\ &= f(((z_i)_i, a) + ((w_i), b)) && \text{by definition of } G \times H \end{aligned}$$

Moreover, this map is surjective, since given any $(z_i)_{i \in \mathbb{N}}$,

$$f((z_1, z_2, z_3, \ldots), z_0) = (z_i)_i.$$

The map f is also injective: if we denote the constant sequence equal to 0 by $\mathbf{0}$, then

$$f((z_i)_i, h) = \mathbf{0} \iff (h, z_0, z_1, \ldots) = \mathbf{0} \iff h = 0 \text{ and } z_i = 0 \text{ for all } i \geqslant 0 \iff ((z_i)_i, h) = 0_{G \times H}.$$

We have established the desired isomorphism. □

[1] Note: this gives us an example of groups G, H such that there is an isomorphism $G \times H \cong G$ but H is nontrivial. Since $G \times H \cong G$ can be rewritten as $G \times H \cong G \times \{e\}$, this shows that in general one cannot cancel groups in isomorphisms between direct products.

Problem 3. Prove that if $f\colon G \to H$ is a group homomorphism and $K \leq H$ then the **preimage** of K, defined as

$$f^{-1}(K) := \{g \in G \mid f(g) \in K\}$$

is a subgroup of G.

Proof. Since f is a homomorphism, $f(e_G) = e_H \in K$, and thus $e_H \in f^{-1}(K) \neq \varnothing$.

If $x, y \in f^{-1}(K)$, then $f(x) \in K$ and $f(y) \in K$. Since f is a homomorphism and K is closed under multiplication and taking inverses,

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} \in K,$$

and thus $xy^{-1} \in f^{-1}(K)$. By the One-step subgroup test, we conclude that $f^{-1}(K)$ is a subgroup of G. □

Problem 4. Let G be a group.

(4.1) Prove that $\mathrm{Aut}(G)$, the set of automorphisms of G, is a group under composition.

Proof. First, we show that composition is an operation on this set: i.e., that the composition of automorphisms is an automorphism. Let $\alpha, \beta \in \mathrm{Aut}(G)$. Then each is bijective, so the composition $\alpha \circ \beta$ is bijective. To check that $\alpha \circ \beta$ is a homomorphism, take $g, h \in G$ and compute

$$\alpha \circ \beta(g \cdot h) = \alpha(\beta(g \cdot h)) = \alpha(\beta(g) \cdot \beta(h)) = \alpha(\beta(g)) \cdot \alpha(\beta(h)) = (\alpha \circ \beta)(g) \cdot (\alpha \circ \beta)(h).$$

Thus, composition is an operation on $\mathrm{Aut}(G)$.

Now, composition of function is associative, so the operation on $\mathrm{Aut}(G)$ is associative. The identity map I on G is an automorphism, and for any $\alpha \in \mathrm{Aut}(G)$, we have $I \circ \alpha = \alpha \circ I = \alpha$, since $(I \circ \alpha)(g) = (\alpha \circ I)(g) = \alpha(g)$ for all $g \in G$.

Finally, the inverse function of an automorphism is an automorphism, since it is also an isomorphism from G to itself; the inverse function is the inverse under composition, and hence an inverse element under the given operation. This completes the verification that $\mathrm{Aut}(G)$ is a group. □

(4.2) For $g \in G$, let $\psi_g : G \to G$ be given by $\psi_g(x) = gxg^{-1}$. Prove that $\{\psi_g \mid g \in G\}$ is a subgroup of $\mathrm{Aut}(G)$.

Proof. We first prove ψ_g is a homomorphism. Given $a, b \in G$, we have

$$\psi_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \psi_g(x)\psi_g(y).$$

Now we claim ψ_g is an automorphism. In fact, $\psi_{g^{-1}}$ is the inverse homomorphism, since $\psi_{g^{-1}}\psi_g(x) = g^{-1}gxg^{-1}g = x$ and $\psi_g\psi_{g^{-1}}(x) = gg^{-1}xgg^{-1} = x$.

Let $H = \{\psi_g \mid g \in G\}$. To show H is a subgroup, note first that H is nonempty since $\psi_e \in H$. We now claim that $\psi_g, \psi_h \in H$, $\psi_g \circ \psi_h = \psi_{gh}$; indeed, for $x \in X$, we have

$$(\psi_g \circ \psi_h)(x) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \psi_{gh}(x),$$

and $\psi gh \in H$, so H is closed for the product. Finally, we also proved already that for all $x \in G$, $(\psi_x)^{-1} = \psi_{x^{-1}} \in H$, so H is closed under inverses. Thus, H is a subgroup of $\mathrm{Aut}(G)$ by the Two-step test. □

Problem 5. Prove[2] Lagrange's Theorem: If G is a finite group, and $H \leq G$ is a subgroup, then $|H|$ divides $|G|$.

Proof. Let H act on G by left multiplication. We show that every orbit of this action has size $|H|$. Indeed, consider $g \in G$ and define a function

$$\begin{aligned} H &\to \mathrm{Orb}_H(g) \\ h &\mapsto hg. \end{aligned}$$

I claim this function is bijective. First, note that it is surjective by construction. To see it is injective, assume $f(h) = f(h')$. Then $hg = h'g$, and by the cancellation property we conclude that $h = h'$, which shows f is injective. Now since f is bijective we conclude that $|H| = |\mathrm{Orb}_H(g)|$.

The orbits for this action form a partition of G. Since G is finite, there are finitely many orbits, so we choose representatives $g_1, \ldots, g_k$ for each distinct orbit, and we have a disjoint union

$$G = \bigcup_{i=1}^{j} \mathrm{Orb}_H(g_i).$$

Therefore we have

$$|G| = \sum_{i=1}^{k} |\mathrm{Orb}_H(g_i)| = \sum_{i=1}^{k} |H| = k|H|,$$

and thus $|H|$ divides $|G|$. □

[2]Hint: Let H act on G by left multiplication: $h \cdot g = hg$. You can use that this is an action without verifying it. Compute the cardinality of each orbit.