415A/515A Exam 2
Practice Problems
(Solutions)

1. Write each of the following as a single cycle or a product of disjoint cycles:

(a.) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 4 & 2 & 1 \end{pmatrix}$ (b.) $(1\ 2)(1\ 3)(1\ 4)$

(c.) $(1\ 3)^{-1}(2\ 4)(2\ 3\ 5)^{-1}$ (d.) $(1\ 4\ 5)(1\ 2\ 3\ 5)(1\ 3)$

Solution.
(a.) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 4 & 2 & 1 \end{pmatrix} = (1\ 3\ 6)(2\ 5)$
(b.) $(1\ 2)(1\ 3)(1\ 4) = (1\ 4\ 3\ 2)$
(c.) $(1\ 3)^{-1}(2\ 4)(2\ 3\ 5)^{-1} = (1\ 3)(2\ 4)(2\ 5\ 3) = (1\ 3\ 4\ 2\ 5)$
(d.) $(1\ 4\ 5)(1\ 2\ 3\ 5)(1\ 3) = (2\ 3)(4\ 5)$

2. How many elements of S_n map n to n?

Solution. An element of S_n which fixes n will permute (or fix) the other $n-1$ integers; hence, be an element of $S_{n-1} \leq S_n$. Thus, there are $|S_{n-1}| = (n-1)!$ elements of S_n which map n to n.

3. Determine the right cosets of $\langle 3 \rangle$ in $\mathbb{Z}_{12}$.

Solution. Since 3 has order 4 in $\mathbb{Z}_{12}$, we know $[\mathbb{Z}_{12} : \langle 3 \rangle] = 12/4 = 3$ and so there will be three cosets. They are given by:

$$\{0, 3, 6, 9\}$$
$$\{1, 4, 7, 10\}$$
$$\{2, 5, 8, 11\}.$$

4. Define the *diagonal subgroup* of $\mathbb{R} \times \mathbb{R}$ to be $H = \{(x, x) : x \in \mathbb{R}\}$ where the operation is addition in each component. Describe the right cosets of H in $\mathbb{R} \times \mathbb{R}$ geometrically.

Solution. Let (a, b) be an arbitrary element of $\mathbb{R}\times\mathbb{R}$, we want to describe the right coset, $H(a, b)$. By definition, $H(a, b) = \{(x, x) + (a, b) : (x, x) \in H\} = \{(x + a, x + b) : x \in \mathbb{R}\}$. Choose any two distinct elements contained in this coset, say $(x_1 + a, x_1 + b)$ and $(x_2 + a, x_2 + b)$, then it's not hard to see the slope of the secant line between them is 1. Thus, any two points in $H(a, b)$ lie on a line of slope 1, and since (a, b) is an element of this coset all other points in the coset like on the line of slope 1 passing through (a, b); more explicitly, $H(a, b) \leftrightarrow y = x - a + b$.

5. Let A and B be groups. Prove that each right coset of $A \times \{e\}$ in $A \times B$ contains precisely one element from $\{e\} \times B$.

Proof. Let $(a_0, b_0) \in A \times B$, and consider the right coset $A \times \{e\}(a_0, b_0) = \{(a + a_0, e + b_0) : a \in A\} = \{(a + a_0, b_0) : a \in A\}$. Since A is a group, $-a_0 \in A$ and hence $(-a_0 + a_0, b_0) = (e, b_0) \in A \times \{e\}(a_0, b_0)$. Clearly $(e, b_0) \in \{e\} \times B$, so it follows that the coset $A \times \{e\}(a_0, b_0)$ contains at least one element of $\{e\} \times B$. (We now need to show that it contains *exactly* one such element.)

Suppose $(e, b_1), (e, b_2) \in \{e\} \times B$ are distinct elements such that $(e, b_1), (e, b_2) \in A \times \{e\}(a_0, b_0)$. Then there exist some $a_1, a_2 \in A$ such that $(a_1, e) + (a_0, b_0) = (e, b_1)$ and $(a_2, e) + (a_0, b_0) = (e, b_2)$. In particular, this implies that $e + b_0 = b_1$ and $e + b_0 = b_2$, which is only possible if $b_0 = b_1 = b_2$; a contradiction since $(e, b_1), (e, b_2)$ are distinct. Thus, any right coset contains precisely one element from $\{e\} \times B$.

□

6. Prove or disprove: The direct product of two cyclic groups is cyclic.

   Solution. This claim is false. Many counterexamples could be given; for instance, $\mathbb{Z}$ is cyclic, but $\mathbb{Z} \times \mathbb{Z}$ is not. Maybe an easier counterexample to verify, $\mathbb{Z}_2$ is cyclic but $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not (the only elements are $(0,0), (0,1), (1,0)$ and $(1,1)$ and it is clear that none of these alone generate the whole group).

7. Prove that if $a, b \in \mathbb{Z}$ then $\langle a, b\rangle = \langle d\rangle$, where $d = (a, b)$ (the greatest common divisor of a and b). Note: The notation $\langle a, b\rangle$ denotes the subgroup generated by the two elements a and b.

   Proof. Since $d = (a, b)$ we know that we may write d as a linear combination of a and b, say $d = an + bm$ for some $n, m \in \mathbb{Z}$. So, d is clearly an element of $\langle a, b\rangle = \{ar + bs : r, s \in \mathbb{Z}\}$, and hence $\langle d\rangle \subseteq \langle a, b\rangle$.

   Now, since d is a divisor of both a and b we may write $a = dk$ and $b = d\ell$ for some integers $k, \ell \in \mathbb{Z}$. Thus a and b are both elements of $\langle d\rangle = \{dt : t \in \mathbb{Z}\}$, and hence $\langle a, b\rangle \subseteq \langle d\rangle$.

   Combining the inclusions we see $\langle a, b\rangle = \langle d\rangle$, as desired. □

8. Compute $[\mathbb{Z}_{40} : \langle 12, 20\rangle]$.

   Solution. We will begin by using the result of Problem 7 above. Since $(12, 20) = 4$ it follows that $\langle 12, 20\rangle = \langle 4\rangle$, so we only need to compute $[\mathbb{Z}_{40} : \langle 4\rangle]$. A quick computation shows $|4| = 10$ in $\mathbb{Z}_{40}$ and hence $|\langle 4\rangle| = 10$. Thus,

$$[\mathbb{Z}_{40} : \langle 12, 20\rangle] = [\mathbb{Z}_{40} : \langle 4\rangle] = \frac{|\mathbb{Z}_{40}|}{|\langle 4\rangle|} = \frac{40}{10} = 4.$$

9. Assume that G is a group with a subgroup H such that $|G| < 45$, $|H| > 10$ and $[G : H] > 3$. Find $|G|, |H|$ and $[G : H]$.

   Solution. Since $[G : H] > 3$ (and $|G| < 45 < \infty$) we know that $\frac{|G|}{|H|} > 3$ and so $|G| > 3|H|$. In particular, since $|H| < 10$, it follows that $|G| > 30$, giving $30 < |G| < 45$. Similarly, since $|G| < 45$ it also follows that $45 > 3|H|$ and so $15 > |H|$, giving $10 < |H| < 15$.

   Since $|G|$ must be an integer, and $|G| > 3|H|$ it follows that $|G| \geq 4|H|$. Now, if $|H|$ is $12, 13$ or 14, then this would imply $|G|$ is greater than or equal to $48, 52$ or 56, respectively; all of which are impossible since $|G| < 45$, thus $|H| = 11$. Using this it is clear that $|G| = 44$ (this insures that the index is large enough while keeping the size of G under 45). So finally, $[G : H] = 4$.

10. Determine the isomorphism class of $\mathbb{Z}_{18}/\langle 3\rangle$.

    Solution. Clearly we have $|\langle 3\rangle| = 6$, so it follows $\left|\mathbb{Z}_{18}/\langle 3\rangle\right| = \left|\frac{\mathbb{Z}_{18}}{\langle 3\rangle}\right| = \frac{18}{6} = 3$. Now, $\mathbb{Z}_{18}$ is cyclic, and we know all subgroups cyclic groups are cyclic, so it follows the subgroup $\mathbb{Z}_{18}/\langle 3\rangle$ is cyclic and of order 3. Thus,

$$\mathbb{Z}_{18}/\langle 3\rangle \cong \mathbb{Z}_3.$$

11. Let G be a simple group with $\phi : G \to G$ any homomorphism. Prove that $\phi(G) \cong \{e\}$ or $\phi(G) \cong G$ (i.e., the image of G under ϕ is either the trivial group or all of G).

    Proof. By the Fundamental Homomorphism Theorem, $\phi(G) \cong G/\ker\phi$, so it suffices to show $G/\ker\phi = \{e\}$ or $G/\ker\phi = G$, i.e., $\ker\phi = G$ or $\ker\phi = \{e\}$, respectively. The kernel of a homomorphism is always a normal subgroup, and since G is simple it follows that $\ker\phi$ is either trivial or the whole group, as desired. □

12. True or False: A homomorphism is surjective if and only if its kernel equals the identity.

Solution. False. A homomorphism is *injective* if and only if its kernel equals the identity. (See Corollary 13.18 for a proof of this fact.)

13. True or False: If $\phi : G \to H$ is a homomorphism, then $\ker \phi$ is a subgroup of G.

Solution. True. (See Corollary 13.20 for a stronger result.)

14. Let $N \lhd G$, prove that if $[G : N]$ is prime, then G/N is cyclic. Does the converse hold?

Proof. We know $|G/N| = [G : N]$ and since this index it prime, G/N is a group of prime order, hence cyclic. □

The converse does not hold. Consider, for example, the group $G = \mathbb{Z}_{12}$ with normal subgroup $N = \mathbb{Z}_3$. Then a simple check shows $G/N \cong \mathbb{Z}_4$, which is clearly cyclic, but $[G : N] = |G/N| = 4$ which is not prime.

15. Prove that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order.

Proof. To prove that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order it suffices to show that for every $d \in \mathbb{Q}$ there exists a finite integer k such that $kd \in \mathbb{Z}$. Let $d = \frac{a}{b} \in \mathbb{Q}$ with $(a, b) = 1$, then clearly $b \in \mathbb{Z}$ and $bd \in \mathbb{Z}$, as desired. (i.e., multiply each fraction by its denominator, which is obviously finite, to obtain an integer – which is trivial in $\mathbb{Q}/\mathbb{Z}$.) □