Homework #9. Due on Thursday, November 7th, 11:59pm on Canvas

Reading:

1. For this assignment: Online lectures 16, 17 (before Cayley's theorem) and the beginning of 18 (just the statement of Lagrange Theorem and its consequences). From Hungerford: 7.4 and beginning 7.5.

2. For next week's classes: Monday, Nov 4: online lecture 17; Wednesday, Nov 6: online lecture 19 and the beginning of lecture 18 (just 18.1). From Hungerford: beginning of 7.5 for Monday's class and 8.1 for Wednesday's class.

Online lectures are currently posted on the Spring 2016 webpage

`https://m-ershov.github.io/3354_Spring2016/`

Problems:

Problem 1: Recall that by Lemma 17.2 in class (not in the online notes), for any homomorphism of groups $\varphi : G \to H$ and any $g \in G$ we have

- (i) $o(\varphi(g)) \leq o(g)$;
- (ii) If $o(g)$ is finite, then $o(\varphi(g))$ divides $o(g)$.

Use (i) to give a short proof of Proposition 15.3 from online notes which asserts that isomorphisms preserve orders of elements, that is, for any isomorphism of groups $\varphi : G \to H$ and any $g \in G$ we have $o(\varphi(g)) = o(g)$.

Problem 2:

- (a) Let G be an abelian group and let m be an integer. Prove that the map $\varphi : G \to G$ given by $\varphi(x) = x^m$ is a homomorphism.
- (b) Let $G = (\mathbb{Z}_{12}, +)$. Define the map $\varphi : G \to G$ by $\varphi([x]) = 3[x] = [3x]$. Prove that φ is a homomorphism and compute its image and kernel.

Problem 3: Let G and H be groups and $\varphi : G \to H$ a homomorphism. For each of the following statements, determine whether it is true (in general) or false (in at least one case). If the statement is true, prove it; if it is false, give a specific counterexample.

- (a) If H is abelian, then G is abelian
- (b) If G is abelian, then H is abelian
- (c) If G is abelian, then $\varphi(G)$ is abelian
- (d) If G is abelian, then $\mathrm{Ker}\,(\varphi)$ is abelian

Problem 4: Let $G = \langle x \rangle$ be a cyclic group generated by some element x and let H be an arbitary group.

(a) Prove that for any $h \in H$ there exists AT MOST one homomorphism $\varphi : G \to H$ with the property that $\varphi(x) = h$, and if such φ exists, it is given by the formula

$$\varphi(x^k) = h^k \text{ for all } k \in \mathbb{Z}. \qquad (***)$$

In other words, a homomorphism from a cyclic group is uniquely determined by where it sends a generator (but there is no guarantee that every choice of the image of a generator can be extended to an homomorphism)

(b) Assume that there exists a (well-defined) map $\varphi : G \to H$ satisfying the formula (***) from (a). Prove that φ is a homomorphism. Note that φ given in (***) may not be well defined since for a given $g \in G$ there may be more than one value of k such that $g = x^k$.

(c) Assume that G is infinite. Prove that for any $h \in H$ there exists a map $\varphi : G \to H$ satisfying (***) for all $k \in \mathbb{Z}$ (Note that φ is a homomorphism by (b))

(d) Now assume that G is finite and let $n = |G| = o(x)$. Fix $h \in H$. Prove that the following are equivalent:

(i) There exists a map $\varphi : G \to H$ satisfying (***) (for your chosen h and all $k \in \mathbb{Z}$)

(ii) $h^n = e$

(iii) $o(h)$ divides n.

(e) Now assume that $G = H = \mathbb{Z}_n$ for some $n \in \mathbb{N}$ (as usual the operation is addition). Use (d) to prove that for any $m \in \mathbb{Z}$ there exists a unique homomorphism $\varphi_m : \mathbb{Z}_n \to \mathbb{Z}_n$ such that $\varphi_m([1]) = [m]$ and write down the explicit formula for it:

$$\varphi_m([k]) = \dots$$

Then prove that φ_m is an isomorphism $\iff gcd(m, n) = 1$.

Problem 5: Let G and H be finite groups such that $|G|$ and $|H|$ are coprime. Prove that any homomorphism $\varphi : G \to H$ must be trivial, that is, $\varphi(x) = e_H$ for all $x \in G$ where e_H is the identity element of H. **Hint:** Use the Range-Kernel theorem (see online Lecture 16; in class we called it the Image-Kernel Theorem) and Lagrange theorem (see Lecture 18) applied to a suitable subgroup.

Problem 6:

(a) Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 3 & 7 & 2 & 6 & 4 \end{pmatrix}$ in two-line notation. Write f as in disjoint cycle form.

(b) Write the following element of S_9 as a product of disjoint cycles:

$$(1, 2, 4, 6, 7)(3, 4, 5, 1, 8)(9, 2, 3, 5)$$

Problem 7: List all elements of S_3 in disjoint cycle form and compute the multiplication table of S_3.

Problem 8: As proved in online Lecture 17, if $f \in S_n$ is written as a product of disjoint cycles $f_1 f_2 \ldots f_r$ where f_1 has length k_1, ..., f_r has length k_r, then the order of f is the least common multiple of $k_1, k_2, \ldots, k_r$. Use this fact to find the smallest $n \in \mathbb{N}$ for which S_n has an element of order 15 and prove your answer (include all the details).

Bonus problem:

(a) Let G be a group and let $\mathrm{Aut}\,(G)$ be the set of all automorphisms of G (= isomorphisms from G to G). Prove that elements of $\mathrm{Aut}\,(G)$ form a group with respect to composition. This group is called the *automorphism group of G*. **Hint:** This follows from Problem 6 of HW#8. What is the identity element of $\mathrm{Aut}\,(G)$?

(b) Let $G = \mathbb{Z}_n$ (with addition). Use the result of Problem 4(e) to prove that $\mathrm{Aut}\,(G)$ is isomorphic to $\mathbb{Z}_n^{\times}$ (with multiplication). **Hint:** This problem is much easier than it seems. Elements of $\mathrm{Aut}\,(G)$ are explicitly described in Problem 4(e). Use it to find a natural bijective mapping between $\mathrm{Aut}\,(G)$ and $\mathbb{Z}_n^{\times}$; then show that your mapping is in fact an isomorphism.