Homework #8. Due Thursday, March 26th

Reading:

1. For this assignment: Section 3.6, class notes (Lectures 15-16) + online supplement on direct products (see webpage).

2. for Tuesday's class: Section 4.1. Read at least up to Example 7.

Problems:

Problem 1:

(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) Now use (a) and a theorem from class to solve Problem 2(a) in HW#6 without doing any computations.

Problem 2: 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 $\text{Ker}\,(\varphi)$ is abelian

Problem 3: 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 range and kernel. This problem is a warm-up for Problem 4.

Practice problem I: Let A and B be finite sets of the same cardinality, that is, $|A| = |B| = n < \infty$. Let $f : A \to B$ be a function. Prove that f is injective if and only if f is surjective.

Problem 4: Fix integers $n > 1$ and $m \geq 1$, and let $G = (\mathbb{Z}_n, +)$. Define the mapping $\varphi_m : G \to G$ by

$$\varphi_m([x]) = m[x] = [mx] \text{ for every } [x] \in \mathbb{Z}_n.$$

(a) Prove that $\varphi_m : G \to G$ is always a homomorphism. **Hint:** you already proved it in this homework.

(b) Prove that $\varphi_m(G)$ is equal to $\langle [m] \rangle$, the cyclic subgroup generated by $[m]$.

(c) Prove that φ_m is an isomorphism if and only if $gcd(m, n) = 1$. **Hint:** By part (a), the question is reduced to checking whether φ_m is bijective. By Practice Problem I it suffices to know when φ_m is surjective. To determine when φ_m is surjective, use (b) and one of the parts of Theorem 14.1.

(d) Now let ψ be an arbitrary **automorphism** of G, that is, ψ is an isomorphism from G to G. Prove that $\psi = \varphi_m$ for some m, with $gcd(m,n) = 1$. **Hint:** Let $m \in \mathbb{Z}$ be such that $\psi([1]) = [m]$. Use the fact that ψ preserves group operation (addition in this case) to show that $\psi([x]) = \varphi_m([x])$ for any $x \in \mathbb{Z}$.

Problem 5: Let $m, n > 1$ be positive integer. For each integer x we denote by $[x]_n \in \mathbb{Z}_n$ the congruence class of x in $\mathbb{Z}_n$ and by $[x]_m \in \mathbb{Z}_m$ the congruence class of x in $\mathbb{Z}_m$. Now try to define a map $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$ by

$$\varphi([x]_n) = [x]_m.$$

(a) (practice) Prove that φ is a homomorphism whenever it is well defined.

(b) Now prove that φ is well defined $\iff$ $m \mid n$. **Hint:** By definition, φ is well defined if and only if the following implication holds for all $x, y \in \mathbb{Z}$:

$$\text{if } [x]_n = [y]_n, \text{ then } [x]_m = [y]_m. \qquad (***)$$

Thus, to prove (b) you need to show the following:

(i) If $m \mid n$, then (***) holds for all $x, y \in \mathbb{Z}$

(ii) If $m \nmid n$, then there exist $x, y \in \mathbb{Z}$ for which (***) does not hold.

(c) Find an injective homomorphism $\varphi : \mathbb{Z}_5 \to \mathbb{Z}_{10}$ (note that φ from (b) would not work as it will not be well defined).

Problem 6: Read the online supplement on direct sums before doing this problem. Note that when A and B are abelian groups written additively (operation denoted by $+$) the notation $A \oplus B$ means the same as $A \times B$.

(a) Prove that $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is isomorphic to $\mathbb{Z}_6$. **Hint:** Since every cyclic group of order k is isomorphic to $\mathbb{Z}_k$, it is enough to prove that $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is cyclic.

(b) Let $m, n \neq 2$ be integers and let $l = LCM(m,n)$ be the least common multiple of m and n. Let $G = \mathbb{Z}_m \oplus \mathbb{Z}_n$. Prove that $l([x],[y]) = ([0],[0])$ for any $([x],[y]) \in G$.

(c) Now prove that $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn} \iff m$ and n are coprime. **Hint:** For the forward direction ("$\Rightarrow$") use contrapositive and (b). For the backward direction find a simple generator for $\mathbb{Z}_m \oplus \mathbb{Z}_n$.

Problem 7: 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 and Lagrange theorem (applied to a suitable subgroup). Lagrange theorem (which will be discussed in class next week) asserts that if A is a finite group and B is a subgroup of A, then $|B|$ divides $|A|$.

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 3 of HW#7. What is the identity element of $\mathrm{Aut}\,(G)$?

(b) Let $G = (\mathbb{Z}_n, +)$. Use the result of Problem 3 to prove that $\mathrm{Aut}\,(G)$ is isomorphic to $(\mathbb{Z}_n^{\times}, \cdot)$. **Hint:** This problem is much easier than it seems. Elements of $\mathrm{Aut}\,(G)$ are explicitly described in Problem 4(c). 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.