Homework #8. Due Thursday, October 28th

Reading:

1. For this assignment: Section 3.6 + online supplement on direct products.
2. for Tuesday's class: Section 4.1. Read at least up to Example 7 on page 196 (inclusive).
3. for Thursday's class: Read the part of Section 4.4 on page 219 (the statement of Lagrange theorem, Corollary 4.14 and Example 5).

Problems:

Problem 1: Definition. Let G be a group and g an element of G. We will say that g *has a square root in* G if there exists $x \in G$ such that $x^2 = g$.

(a) Suppose that $\varphi : G \to H$ is a group homomorphism, and suppose that an element $g \in G$ has a square root in G. Prove that $\varphi(g)$ has a square root in H.

(b) Now let $G_1 = (\mathbb{R}^*, \cdot)$ and $G_2 = (\mathbb{R}, +)$. Find all elements of G_1 which have square roots and all elements of G_2 which have square roots. **Warning:** Since the group operation in G_2 is $+$, the notion of a square root in G_2 does not coincide with the usual one.

(c) Recall that we proved in Lecture 15 that the groups G_1 and G_2 are not isomorphic. Use (a) and (b) to give a different proof of this fact.

Problem 2: Problem 3.6.5. **Note:** An epimorphism is a surjective homomorphism. This problem is a warm-up for Problem 3.

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 3: 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

(b) Prove that $\varphi_m(G)$ coincides with $\langle [m] \rangle$, 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 4: 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).

Practice problem II: Problem 3.6.1 (b)(d)(f)(h).

Problem 5: Let G and H be groups and $\varphi : G \to H$ a homomorphism.

(a) Prove that $\varphi(G)$ is a subgroup of H.

(b) Let $y \in \varphi(G)$, and choose some $x_0 \in G$ such that $\varphi(x_0) = y$. Suppose we are given another element $x \in G$. Prove that the following two conditions are equivalent:

(i) $\varphi(x) = \varphi(x_0)$, that is, $\varphi(x) = y$

(ii) there exists $k \in \operatorname{Ker} \varphi$ such that $x = kx_0$.

Hint: The implication (ii)⇒(i) is easy. For the implication (i)⇒(ii), if $\varphi(x) = \varphi(x_0)$, what can you say about $\varphi(xx_0^{-1})$?

(c) Prove that φ is injective $\iff$ $\operatorname{Ker}\varphi = \{e\}$. **Hint:** You can deduce (c) from (b), but it may be more convenient to give a direct proof.

(d) Suppose now that both G and H are finite. Use part (b) to prove the Range-Kernel theorem:

$$|G| = |\operatorname{Ker}\varphi| \cdot |\varphi(G)| \qquad (***)$$

Hint: $|G|$ is the total number of inputs, and $|\varphi(G)|$ is the total number of outputs. Part (b) tells you how many inputs x correspond to each output y.

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 relatively prime. **Hint:** For the forward direction ("$\Rightarrow$") use contrapositive and (b). For the backward direction find a simple generator for $\mathbb{Z}_m \oplus \mathbb{Z}_n$.

Bonus problem:

(a) Let G be a group and let $\operatorname{Aut}(G)$ be the set of all automorphisms of G (= isomorphisms from G to G). Prove that elements of $\operatorname{Aut}(G)$ form a group with respect to composition. This group is called the *automorphism group of* G. **Hint:** This follows from 3.5.1 and 3.5.2. What is the identity element of $\operatorname{Aut}(G)$?

(b) Let $G = (\mathbb{Z}_n, +)$. Use the result of Problem 3 to prove that $\operatorname{Aut}(G)$ is isomorphic to $(\mathbb{Z}_n^*, \cdot)$. **Hint:** This problem is much easier than it seems. Elements of $\operatorname{Aut}(G)$ are explicitly described in Problem 3(c). Use it to find a natural bijective mapping between $\operatorname{Aut}(G)$ and $\mathbb{Z}_n^*$; then show that your mapping is in fact an isomorphism.