MODERN ALGEBRA I GU4041

Homework 9, due November 9: Classification of abelian groups

In what follows, two groups of order N are said to be in the same *isomorphism class* if they are isomorphic. So for any prime number p, when we say there is only one isomorphism class of groups of order p, we mean every group of order p is isomorphic to a cyclic group of order p. On the other hand, for example, there are exactly two isomorphism classes of groups of order 4: $\mathbb{Z}_4$ and K_4.

The term is used loosely: if we have a set S of abelian groups of order N, we can define an equivalence relation on S by saying that the groups G, G' in S are equivalent if they have the same order: $|G| = |G'|$. So you can imagine in problems 1 and 3 below that you have a set S containing ALL abelian groups of the given orders, and an isomorphic class is an equivalence class for this relation. Strictly speaking, however, there is no such set, because of considerations like Russell's paradox. But that shouldn't constrain your imagination.

1. List the isomorphism classes of abelian groups of the following orders: 27, 200, 605, 720.

(More precisely, for each of the orders N, give a list of abelian groups of order N such that any abelian group of order N is isomorphic to one of the groups on your list. You should use the same interpretation in problem 3.)

2. Judson, section 13.4, exercises 6, 8. In problem 8, "not true in general" means "not necessarily true if G, H, K are not assumed to be abelian.

3. Find the smallest integer $n > 42$ such that there is exactly one isomorphism class of abelian groups of order n and exactly one isomorphism class of abelian groups of order $n+1$. Justify your answer, including why there is no smaller n.

4. Let $n > 1$ and $m > 1$ be integers. In the next question, we recall that if $a \in \mathbb{Z}$ and $x \in \mathbb{Z}_n$, we can define $ax \in \mathbb{Z}_n$ by letting $\tilde{x}$ be any element of $\mathbb{Z}$ with residue class x modulo n and letting ax denote the residue class of $a\tilde{x}$ modulo n.

(a) Show that if a and d are integers such that $(a, n) = (d, m) = 1$, then there is an automorphism

$$\alpha_{a,d} : \mathbb{Z}_n \times \mathbb{Z}_m \xrightarrow{\sim} \mathbb{Z}_n \times \mathbb{Z}_m$$

such that, for all $(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_m$,

$$\alpha_{a,d}((x, y)) = (ax, dy).$$

(b) Suppose $(n,m)=1$. Show that the group $\mathbb{Z}_{nm}$ has a unique subgroup A_n of order n and a unique subgroup A_m of order m. Write down an isomorphism

$$A_n \times A_m \xrightarrow{\sim} \mathbb{Z}_{nm}.$$

(c) If $(n,m)=1$, show that any automorphism of $\mathbb{Z}_n \times \mathbb{Z}_m$ is of the form $\alpha_{a,d}$ where a and d are as in part (a).

(d) Write down an automorphism of $\mathbb{Z}_3 \times \mathbb{Z}_9$ that is *not* of the form $\alpha_{a,d}$.

(e) Suppose $a,b,c,d \in \mathbb{Z}$. Let $M : \mathbb{Z}_3 \times \mathbb{Z}_3$ be the function

$$M(x,y) = (ax+by, cx+dy).$$

For what a,b,c,d is this M an automorphism?

Recommended reading

Judson, Section 13.1.