Lesson 18

THE FUNDAMENTAL THEOREM OF FINITE ABELIAN GROUPS

We want to mention the *Fundamental Theorem of Finite Abelian Groups* at this point even though we will defer a proof of it until much later. Basically, this theorem says that every finite abelian group can be written as a direct product of cyclic subgroups of orders consisting of various prime numbers raised to various powers.

Theorem: If G is a finite abelian group, then G is isomorphic to the direct product of cyclic groups where each cyclic group has order equal to the power of a prime number. In other words, $G \cong \mathbb{Z}_{p_1^n} \times \mathbb{Z}_{p_2^m} \times \ldots \times \mathbb{Z}_{p_j^k}$ where $p_1, p_2, \ldots p_j$ are prime numbers and $n, m, \ldots k$ are positive integer powers.

Though we won't give a proof of this until later, the theorem makes a certain amount of intuitive sense. First note that if A and B are two normal subgroups of G such that $A \cdot B = G$ and $A \bigcap B = e$, the identity, then we can say that G is isomorphic to the direct product of A and B, $G \cong A \times B$. Note also that every subgroup of an abelian group is automatically a normal subgroup. Now pick an arbitrary element a in G and look at the order of the cyclic subgroup that a generates. If that order is equal to a prime number raised to a power, then fine. Otherwise, if its order is a number that is a product of two or more primes, then we can rewrite it as a direct product of two or more cyclic subgroups of prime power order. For example, if the order of our cyclic subgroup is six, then we can rewrite this as a direct product of a cyclic group of order two and a cyclic group of order three. In other words, $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. So anyway, we can pick an arbitrary element in G and generate the first term(s) in the direct product we are going to construct. Now pick a second element in G such that the cyclic subgroup it generates has no elements, other than the identity, in common with the first subgroup generated. This second subgroup can also be written as a direct product of groups of prime power order, and we add its factors to the first. And now we just continue this process until we arrive at a direct product that is equal to the original group G. Well, the argument I've just given is not ironclad, and there are many details that must be paid attention to in order to arrive at a proper proof, but hopefully this argument makes the conclusion look very plausible.

A consequence of this theorem is that for any given positive integer, we can determine just how many abelian groups of that order exist, and we can represent each one as a direct product of cyclic groups of prime power order. For example, since 9 can also be written as $3 \cdot 3$, there are essentially two nonisomorphic abelian groups of order 9, namely, $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$.