Algebra 1 Homework 7
Lee Fisher
2017-10-8

5.2 #1: Find the isomorphism classes of abelian groups of order 200.

Here are the isomorphism classes, from the fundamental theorem of finitely generated Abelian Groups:

$$\begin{aligned} G &\cong \mathbb{Z}_{200} \\ &\text{or } \mathbb{Z}_{100} \times \mathbb{Z}_2 \\ &\text{or } \mathbb{Z}_{50} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\ &\text{or } \mathbb{Z}_{40} \times \mathbb{Z}_5 \\ &\text{or } \mathbb{Z}_{20} \times \mathbb{Z}_{10} \\ &\text{or } \mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_2 \end{aligned}$$

From the divisibility restriction, these are all of the factors.

5.2 #2: Find the invariant factors and the elementary divisiors of the abelian group.

$$G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5.$$

For finding the elementary divisors we can see that G has been decomposed into a direct product of prime power cyclic subgroups. So the elementary divisors are in this order: 2, 2, 2, 9, 5, and 5.

To find the invariant factors we can combine cyclic groups that share no common factors to be the cyclic group on the product, then we have that

$$G \cong \mathbb{Z}_{90} \times \mathbb{Z}_{10} \times \mathbb{Z}_2.$$

Which concludes this problem.

5.2 #4: Let G be a finite group and p a prime factor of $|G|$. Prove that the number of order p elements in G is congruent to -1 modulo p.

Consider solutions in G to $x_1 x_2 \cdots x_p = 1$, There are $|G|^{p-1}$ such solutions. That is you can choose any element from G that you want from the first $p-1$ elements and you must choose the unique inverse of the product of those elements to be x_p. Since p divides $|G|$, p also divides $|G|^{p-1}$. If $(x_1, x_2, \ldots, x_p)$ is a solution then any cyclic permutation of $(x_1, x_2, \ldots x_p)$ is a solution because if you have one solution then you have $x_2 \cdots x_p = x_1^{-1}$ which means that $x_2 \cdots x_p x_1 = 1$ is also a solution.

If $(x_1, x_2, \ldots, x_p)$ is a solution where at least two elements differ then the cyclic permutations of this solution give you p different solutions. So the number of solutions to $x_1 x_2 \cdots x_p = 1$ with not all x_i equal is a multiple of p. Therefore the number of solutions with x_i all equal is a difference of two multiples of p, this means it must be a multiple of p.

The number of solutions to $x^p = 1$ is congruent to 0 mod p. Solutions to this equation are order p elements, since p is a prime, and the identity element. So the number of order p elements is congruent to -1 mod p.

5.3 #2: Let G be a finite group and $N_1, ..., N_n$ normal subgroups of G such that $G = N_1 \cdots N_n$ and $|G| = |N_1| \cdots |N_n|$. Prove that G is the internal direct product of G.

We know that G is the internal direct product of all the N_i if and only if it is isomorphic to the external direct product of the N_i. Consider the map:

$$\phi : N_1 \times N_2 \cdots \times N_n \to G$$

By $\phi((m_1, \ldots, m_n)) = m_1 m_2 \ldots m_n$. ϕ is a homomorphism because,

$$\begin{aligned} \phi((m_1, \ldots m_n)(k_1, \ldots, k_n)) &= \phi(m_1 k_1, m_2 k_2, \ldots m_n k_k) \\ &= m_1 k_1 \cdots m_n k_n \\ \text{Since the } N_i \text{ are normal: } &= m_1 \cdots m_n k_1 \cdots k_n \\ &= \phi(m_1, \ldots, m_n)\phi(k_1, \ldots, k_n) \end{aligned}$$

This homomorphism is surjective because $G = N_1 \cdots N_n$. Suppose for sake of contradiction that ϕ is not 1-1, this would mean that two different elements in the external direct product multiply to be the same element in G, and since both groups are finite and ϕ is surjective, this implies that $|N_1||N_2| \cdots |N_n| = |N_1 \times N_2 \cdots N_n| > |G|$, but this contradicts the assumption that $|G| = |N_1||N_2| \cdots |N_n|$. So ϕ must be 1-1, and therefore, an isomorphism. So G is isomorphic to the external direct product, and must be the internal direct product of the N_i.

5.5 #1: Prove Proposition 5.16.

Proposition 5.16 Let G be a group, H, K subgroups of G, and $H \trianglelefteq G$. Let $\varphi : K \to Aut(H)$ be the homomorphism associated with the conjugate action of K on H. Then the following statements are equivalent:

1. $\phi : H \rtimes_\varphi K \to G$ defined by $\phi(h, k) = hk$ is an isomorphism.
2. Every element $g \in G$ can be written as $g = hk$ with $h \in H$ and $k \in K$ in a unique way.
3. $G = HK$ and $H \cap K = \{e\}$.

$1 \to 2$ Since ϕ is an isomorphism from $H \rtimes_\varphi K \to G$ every element in G is a unique product of elements in the semi-direct product. But every element in the semi-direct product is an element in $H \times K$, (only the multiplication operation is different, not the elements) so every element $g \in G$ is a unique product of elements hk with $h \in H$ and $k \in K$.

$2 \to 3$ Since every element in G can be written as $g = hk$ with $h \in H$ and $k \in K$ this gives us that $G = HK$. Also suppose there is an $aH \cap K$ with $a \neq e$. This means that if $g = hak$ then $g = (ha)k = h(ak)$, which contradicts the uniqueness of the representation of g as a product of elements in H and K. So $H \cap K = \{e\}$.

$3 \to 1$ Suppose $G = HK$ and $H \cap K = \{e\}$. Let consider a map ϕ which sends $H \rtimes_\varphi K$ to G by $\phi((h, k)) = hk$.

This is a homomorphism because:

$$\begin{aligned} \phi((h_1, k_1)(h_2, k_2)) &= \phi((h_1 k_1 h_2 k_1^{-1}, k_1 k_2)) \\ &= h_1 k_1 h_2 k_1^{-1} k_1 k_2 \\ &= h_1 k_1 h_2 k_2 \\ &= \phi((h_1, k_1))\phi((h_2, k_2)) \end{aligned}$$

This homomorphism is surjective because $G = HK$. Now consider $Ker(\phi)$, these are elements $h \in H$ and $k \in K$ such that $hk = 1$ these are elements in H and K separately whose inverses lie in the other group. This means one of the pairs must lie in the subgroup $H \cap K$ and the other element must be it's

inverse. However, $H \cap K$ is just the identity element, so $Ker(\phi)$ is just the element (e, e). Thus ϕ is also 1-1, and therefore it must be an isomorphism.

5.5 #4 (a): For any positive integer n, prove that $Aut(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$.

Let ϕ be an automorphism of Z_n. Since ϕ is a homomorphism, if $m \in \mathbb{Z}_n$ then $\phi(m * 1) = m\phi(1)$. So all of the homomorphisms are completely determined by where they send the element 1 in $\mathbb{Z}_n$. In order for it to be an automorphism it is necessary that is sends the element 1, which generates $\mathbb{Z}_n$, to another generator of $\mathbb{Z}_n$. Also since cyclic groups are completely determined by their only generator, this is a sufficient condition as well. Thus: $\phi \in Aut(\mathbb{Z}_n) \iff \phi(1) \in \mathbb{Z}_n^\times$.

The map φ that sends $\phi(x) = gx \in Aut(\mathbb{Z}_n)$ to $g \in \mathbb{Z}_n^\times$ is one to one and onto because of the previous argument. It is homomorphism as well: $\varphi(\phi_1 \circ \phi_2) = \varphi(g_1 g_2 x) = g_1 g_2 = \varphi(\phi_1)\varphi(\phi_2)$.

5.5 #4 (b): For any primes $p < q$, if $p \mid q - 1$, there exists a monomorphism $\varphi : \mathbb{Z}_p \to Aut(\mathbb{Z}_q)$ and $\mathbb{Z}_q \rtimes_\varphi \mathbb{Z}_p$ is a non-abelian group of order pq.

Since $Aut(\mathbb{Z}_q)$ is isomorphic to $\mathbb{Z}_q^\times$ and p is a prime divisor of $q - 1 = |\mathbb{Z}_q^\times|$, there is an element g of order p in $Aut(\mathbb{Z}_q)$. Consider the map:

$\varphi : \mathbb{Z}_p \to Aut(\mathbb{Z}_q)$

By $\varphi(n) = g^n$. This is a homomorphism because $\varphi(n_1 + n_2) = g^{n_1+n_2} = g^{n_1} g^{n_2} = \varphi(n_1)\varphi(n_2)$. Also consider $Ker(\phi)$, these are $n \in \mathbb{Z}_p$ such that $g^n = Id$. Since g has order p, this means $Ker(\phi) = \{0\}$, so the map is one to one.

We also know that since φ is a nontrivial homomorphism, we know that $\mathbb{Z}_q \rtimes_\varphi \mathbb{Z}_p$ is a non-abelian group of order pq. Because the semidirect product of two Abelian groups is only Abelian if the homomorphism is trivial, and the order the semidirect product is the product of the orders of the groups.

Page 186 #11: Classify groups of order 28 (there are four isomorphism types).

So, $28 = 2^2 \cdot 7$. Consider the number of Sylow 7-subgroups, n_7. We have $n_7 = 1 \bmod 7$ and $n_7 | 4$ so $n_7 = 1$. This tells us that a group of order 28 is a semidirect product of a group of order 4 with the cyclic group of order 7.

If H is a group of order 4 and $\varphi : H \to Aut(\mathbb{Z}_7)$. Since the image of $|H|/|Ker(\varphi)|$ must a divisor of $Aut(\mathbb{Z}_7)$ which has order 6, we know that $|Ker(\varphi)| = 2$ or the Kernel is trivial. If the kernel is trivial then we have that $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_7$ or that $G = \mathbb{Z}_4 \times \mathbb{Z}_7$. If the kernel of φ has order 2 then we have two more cases. Either $H = \mathbb{Z}_2 \times \mathbb{Z}_2$ or $H = \mathbb{Z}_4$.

For the first case we note that inversion (multiplication by 6) is the only automorphism of $\mathbb{Z}_7$ with order 2. Then we consider a map from H to $Aut(\mathbb{Z}_7)$ with a Kernel of order 2. Then we have $\varphi : (0, 0) \to Id$ and φ sends two of $(1, 0)$ $(0, 1)$ or $(1, 1)$ to $-Id$, and the last one of the 3 goes to Id again. However permuting $(1, 0)$, $(1, 1)$, and $(0, 1)$ are all automorphisms of $\mathbb{Z}_2 \times \mathbb{Z}_2$ so it does not matter which two of the elements go to $-Id$, because the semidirect products defined by each choice will all be isomorphic.

Now we consider the homomorphism from $\mathbb{Z}_4 \to \mathbb{Z}_7$. This map must be $\varphi(0) = \varphi(2) = Id$ and $\varphi(1) = \varphi(3) = -Id$. With all of this said there are four non-isomorphic groups of order 28 and they are:

$\mathbb{Z}_4 \rtimes_\varphi \mathbb{Z}_7$, $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_\varphi \mathbb{Z}_7$, $\mathbb{Z}_4 \times \mathbb{Z}_7$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_7$.