# Abstract Algebra

August, Evelyn

11/16/2021

problem What are the elements of $< [5], [3] > \in U(12) \oplus \mathbb{Z}_9$?

solution They are $(5,3), (1,6), (5,0), (1,3), (5,6), (1,0),\ (1,0)$ being the identity element in there.

problem Find an example of an external direct product of cyclic groups that is not cyclic

solution Take for example $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. By the theorems of external direct product, since 2 and 2 (the order of $\mathbb{Z}_2$) are not relatively prime, it follows that $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is not cyclic. Hence we have an example of a non-cyclic Abelian group written as the external direct product of two cyclic groups.

problem 26 Express the group $G = \{1, 7, 23, 49, 55, 65, 71\}$ under multiplication modulo 96 as both the internal direct product of cyclic groups, as well as the external direct product.

solution First, note that $|G| = 8 = 2^3$, hence $G$ is of prime power order. Furthermore, $G$ is Abelian, as multiplication modulo 96 is commutative. We proceed by the Greedy Algorithm for Abelian Groups of Groups of Order $p^k$.
First, we use brute force calculation to find that the orders of the elements of $G$ are $1, 4, 2, 4, 2, 4, 2, 4$ in the same order in which the elements were written in the definition of $G$.

Next, we choose an element of maximal order, which would be order 4. Why not 7, whose order is 4. Computing the cycle for 7, we have $< 7 >= \{7, 49, 55, 1\}$. Call $G_1 =< 7 >$

Now we chose an element of order less than or equal to $|G|/|G_1| = 8/4 = 2$, and not in $< 7 >$. How about 17. We now let $G_2 =< 7 > \times < 17 >$.

Finally, note that $|G| = 8 = | < 7 > \times < 17 > | = 4 * 2$, as $< 7 > \times < 17 > \cong < 7 > \oplus < 17 >$, whose order is $| < 7 > | * | < 17 > | = 8$, since order is preserved under isomorphism. By the steps of the Greedy Algorithm, we stop here, concluding that $G =< 7 > \times < 17 >$.
Also, since $| < 7 > | = 4$, and $| < 17 > | = 2$, these are isomorphic to $\mathbb{Z}_4$ and $\mathbb{Z}_2$ respectively. Hence $G$ is isomorphic to $\mathbb{Z}_4 \oplus \mathbb{Z}_2$.

problem 31 Suppose that $G$ is an Abelian group of order 16. Suppose that there are two elements $a$ and $b$ in $G$ such that $|a| = |b| = 4$, and $a^2 \neq b^2$. Determine the isomorphism class of $G$.

proof for 31 We want to show that $G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$. We will first show that $G =< a > \times < b >$, and then since $< a > \times < b > \cong < a > \oplus < b >$, and since $< a > \cong \mathbb{Z}_4$ and $< b > \cong \mathbb{Z}_4$ (as are all cylcic groups of order 4), it follows that $G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$ and $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ is the isomorphism class of $G$.

First, to show that $G =< a > \times < b >$, we need to show that $< a > \cap < b >= \{e\}$ and $< a >< b >= G$ (since $G$ is abelian, $< a >, < b > G$). We'll start by showing $\{e\} =< a > \cap < b >$.

Let $x \in < a > \cap < b >$. Then by the fundamental theorem of finite cyclic groups it follows that there are four cases for the order of $x$: $|x| = 1$, $|x| = 2$, and $|x| = 4$.

Suppose $|x| = 1$, then $x = e$. Suppose that $|x| = 2$. Then $x = a^2 = b^2$, as these are the only possible ways to have an element of order 2 in $< a >$ and $< b >$. But $a^2 \neq b^2$, hence $x \neq x$, a contradiction. Suppose that $|x| = 4$. Then there are two options for $x$ in $< a >$, $x = a$ and $x = a^3$. Furthermore, there are two options for $x$ in $< b >$, $x = b$ and $x = b^3$. Suppose $x = b = a$. This can't be, because $a^2 \neq b^2$, which implies that $a \neq b$. Suppose $x = a = b^3$. Then $a^4 = ba = e$, in which case $b = a^{-1}$. But then $a^2b = a$ and $b^2a = b$. Then we have $b^2a^2b = b$. By operating $b^2$ on the left of both sides of the equation, we get: $a^2b = b^2b$ then $a = b^2b$. But then $a^2 = b^2ba = b^2$, a contradiction to our supposition.

Suppose $x = a^3 = b^3$. Then $a^3 = b^2b$, hence $a^3b = b^4 = e$. Hence $b^{-1} = a^3 = b^3$. Then $a^6 = a^{6 \mod 4=2} = (a^3)^2 = (b^{-1})^2 = (b^3)^2 = b^6 = b^{6 \mod 4} = b^2$. Hence $a^2 = b^2$, contradicting our supposition that $a^2 \neq b^2$. Hence the only way for $x$ to be in $< a > \cap < b >$ is for $x = e$. Hence $< a > \cap < b >= \{e\}$.

Now we need to show that $< a >< b >= G$. By closure, it suffices to show that there are sixteen elements in $< a >< b >$. Let y be an arbitrary element in $< a >< b >$, then $y = kl$ for some $k \in < a >, l \in < b >$. Suppose $kl = ky$ for $l \neq y$. Then by left cancellation $y = z$, hence each of these options is distinct. Then there are 4 different distinct options for $k$ and 4 different ones for $l$, thus we have $4 \cdot 4 = 16$ options for $y$. Thus, $| < a >< b > | = |G|$. Hence by closure it follows that $< a >< b >= G$.

Having shown that all of the necessary requirements are met, it follows that $< a > \times < b >= G$. Furthermore, by a theorem it follows that $< a > \times < b > \cong < a > \oplus < b >$. Since $< a >, < b >$ are cyclic groups of order 4, it follows that both of them are isomorphic to $\mathbb{Z}_4$. Hence $G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$. Q.E.D.

problem 38 Determine the isomorphism class of $\mathrm{Aut}(\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5)$

solution First, by Sunzi's theorem it follows that, since $2, 3, 5$ are all relatively prime, $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus Z_5 \cong \mathbb{Z}_{30}$. Since isomorphism preserves all of the structure of the group, $\mathrm{Aut}(\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5) \cong \mathrm{Aut}(\mathbb{Z}_{30})$. Furthermore, by Gauss's cool fact, it follows that $\mathrm{Aut}(\mathbb{Z}_{30}) \cong U(30)$.

Now we write out the elements of $U(30)$ (there are $\phi(30) = 8 = 2^3$ of them, hence we can use the Greedy Algorithm for Abelian groups of prime power order):

$$U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}.$$

The orders of these elements in $U(30)$ are, in the same order, $1, 4, 2, 4, 4, 2, 4, 2$. First, we pick a maximum order element, how about 7, and let $G_1 =< 7 >$. Now we pick another element of order less than or equal to the order of $U(30)$ divided by the ordder of $< 7 >$, aka 2, why not 11, whose order is 2. Since the order of $| < 11 > || < 7 > | = 8$, we now stop, finding that $U(30) =< 7 > \times < 11 >$.
Furthermore, by another theorem it follows that $U(30) =< 7 > \times < 11 > \cong < 7 > \oplus < 11 >$. Since $< 7 >$ is a cyclic group of urder 4, and $< 11 >$ of order 2, it follows that $< 7 > \cong \mathbb{Z}_4$ and $< 11 > \cong \mathbb{Z}_2$. Hence, since isomorphism is an equivalence relation hence transitive, $\mathrm{Aut}(\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5) \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2$; this is the isomorphism class we want.

problem 14 (extra credit) Given an Abelian group $G$ such that $n||G|$, it follows that if $n$ is square free, then $G$ has a cyclic subgroup of order $n$.

proof Suppose that $G$ is an Abelian group of order $m$, and suppose that $n$ is a positive square free integer such that $n|m$. By the fundamental theorem of arithmetic and the definition of square free it follows that $n = p_1 \dots p_k$ for distinct primes $p_1, \dots, p_k$ (or $n = 1$, but this is trivial and debatable [at least I think its debatable] not square free). By definition of divisibility, $p_i||G|$ for each $p_i \in \{p_1, \dots, p_k\}$.

By Cauchy's theorem it follows that there exists some element in $G$ of order $p_1$, call it $a_1$. Hence there is a subgroup $< a_1 >$ of $G$ of order $p_1$. Likewise, for each $p_i$.

Consider the set $H =< a_1 > \cdots < a_k >$. By the closure of $G$, and since $H$ is finite, it follows by the finite subgroup test that $H \leq G$. Furthermore, note that since $G$ and hence $H$ are Abelian, it follows that each of these cycles is a normal subgroup of $H$. We want to show that $H =< a_1 > \times \cdots \times < a_k >$. To do so, we need to first show that the intersection $< a_1 > \cap \cdots \cap < a_k >= \{e\}$, where $e$ is the identity in $H$ (as well as in $G$). The second requirement that $H =< a_1 > \cdots < a_k >$ follows directly from the construction of $H$.

Suppose that $a$ is in any two cycles, $< a_i >, < a_j >$, $i \neq j$. By definition of cyclic groups, $a = a_i^m = a_j^n$ for integers $m$ and $n$. Since $|a_i| = p_i$ and $|a_j| = p_j$, we know from a theorem about cyclic groups that, $|a| = p_i / \gcd(p_i, m) = p_j / \gcd(p_j, n)$. Since $p_i$ is prime, there are two cases for $\gcd(p_i, m)$: either $\gcd(p_i, m) = 1$ or $\gcd(p_i, m) = p_i$. Suppose the first case. Then it follows that $|a| = p_i$. But then, multiplying by $\gcd(p_j, n)$ on both sides, we have $p_j = p_i \gcd(p_j, n)$. Then $p_i | p_j$, a contradiction. Hence $\gcd(p_i, m) = p_i$. Thus we see that $|a| = p_i/p_i = 1$, hence $a = e$. Thus the intersection of any cycles must be $\{e\}$. Applying this to each possible cycle, we find that $< a_1 > \cap \cdots \cap < a_k >= \{e\}$.

Since $H =< a_1 > \cdots < a_k >, < a_1 >, \dots, < a_k > \triangleright H$, and $< a_1 > \cap \cdots \cap < a_k >= \{e\}$, it follows that $H =< a_1 > \times \cdots \times < a_k >$. By a theorem, $H =< a_1 > \times \cdots \times < a_k > \cong < a_1 > \oplus \times \oplus < a_k >$. Since $p_1 = | < a_1 > |, \dots p_k = | < a_k > |$ are all distinct primes, it follows that they are pairwise relatively prime, hence $< a_1 > \oplus \times \oplus < a_k >$ is cyclic (and since $< a_i >$ is cyclic for all $i$, but this goes without saying). By properties of external direct products it follows that

$$| < a_1 > \oplus \times \oplus < a_k > | = | < a_1 > | \dots | < a_k > | = |a_1| \dots |a_k| = p_1 \dots p_k = n.$$

Since isomorphism preserves group order, it follows that $|H| = n$. Furthermore, since cyclicness is preserved under isomorphism, it follows that $H$ is cyclic. Since $H$ is a subgroup of $G$, it follows that $G$ has a cyclic subgroup of order $n$.

Hence, given an Abelian group $G$ of order $n$, and a positive, square-free divisor of $m$, $n$, there is a subgroup $H \leq G$ such that $|H| = n$.

corollary (a lower bound for the number of subgroups of an abelian group). Let $G$ be an abelian group such that $|G| = n > 1$. Let $\nu(n)$ denote the number of prime divisors of $n$. Let $Sub(G)$ denote the number of subgroups of $G$. Then

$$Sub(G) \geq 1 + \sum_{i=0}^{\nu(n)} \frac{\nu(n)!}{i!(\nu(n) - i)!}.$$

proof Let $G$ be an abelian group of order $n$. Then by the previous theorem, it follows that every square free divisor of $m|n$ must have at least one corresponding subgroup of that order. By the fundamental theorem of algebra $p_1^{a_1} \dots p_k^{a_k} = n$ for distinct primes $p_1, \dots, p_k$ and positive integers $a_1, \dots, a_k$. Each square free divisor of $n$ will be some combination of these $p_i$s. Then for each possible combination up to $v(n)$ and including the trivial subgroup, there will be a distinct square free divisor. Furthermore, this does not count the group itself, so we add one. Q.E.D.

interesting thoughts we don't have time to think about The upper bound should be the amount of positive divisors of $n$. Something interesting would be to see if someone could make some connections between number theory and groups, on the more analysis side. Like one question could be given any number, and any divisor of that number, what's the probability that that divisor is the order of a subgroup for a random Abelian group of that order.

problem 21 (extra credit) The set $S = \{1, 9, 16, 22, 29, 53, 74, 79, 81\}$ is a group under multiplication modulo 91. Find its isomorphism class.

solution Since $|S| = 9 = 3^2$, it is of prime power order, so we can apply the greedy algorithm. First, we list the orders of these elements: 1:1, 9:3, 16:3, 22:3, 29:3, 53:3, 74:3, 79:3, 81:3. Since 3 is the maximum order, choose an element of order 3, how about 9. We now define $G_1 =< 9 >$. Now we find an element of order less than or equal to $|S|/|9| = 3$ that is not in the cycle of $< 9 >= \{9, 81, 1\}$. Chose 29. Define $G_2 =< 9 > \times < 29 >$ Since $|29| = 3$, and $|29||9| = 3 * 3 = 9 = |S|$, we stop here with $S = G_2 =< 9 > \times < 23 >$. By one of the theorems about external direct products, $S =< 9 > \times < 29 > \cong < 9 > \oplus < 29 >$. Since $< 9 >$ and $< 29 >$ are both cyclic groups of order 3, it follows by another theorem that $< 9 >, < 29 > \cong \mathbb{Z}_3$. Hence the isomorphism class of $S$ is $\mathbb{Z}_3 \oplus \mathbb{Z}_3$.