Abstract Algebra

August, Evelyn

10/26/2021

39: proposition Let $G = \{3^m 6^n : m, n \in \mathbb{Z}\}$ under multiplication. Then G is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$.

proof It isn't immediately clear, at least to me, that G is a group. Clearly it is nonempty. The identity is 1, as $1 \cdot 3^m 6^n = 3^m 6^n$. Inverses are simply the negatives of the exponents. Closure is clear as well. Associativity is inherited from the associativity of integer multiplication. So yes, this is a group.

Consider the function $\phi : G \to \mathbb{Z}$ defined $\phi(a) = (v_3(a) - v_2(a), v_2(a))$, where $v_3, v_2 : \mathbb{Q} \to \mathbb{Z}$ is the p-adic function for primes three and two, extended to the rationals. These functions map each rational number to the difference of the power of the respective prime number in the relatively prime numerator and denominator. For example, $v_3(1/3) = 0 - 1 = -1$ because 3 appears no times in the prime factorization of the denominator, and once in denominator. The function ϕ is bijective, but only because of the restriction of the domain to G.

Before starting anything, we need to show that ϕ is well defined. Take two elements in range of ϕ, $\phi(3^{m_1}6^{n_1})$ and $\phi(3^{m_2}6^{n_2})$ such that $\phi(3^{m_1}6^{n_1}) = \phi(3^{m_2}6^{n_2})$. We want to show that the preimages of these elements are the same. By definition of ϕ we have

$$(v_3(3^{m_1}6^{n_1}) - v_2(v_3(3^{m_1}6^{n_1}), v_2(3^{m_1}6^{n_1})) = ((v_3(3^{m_2}6^{n_2}) - v_2(v_3(3^{m_2}6^{n_2}), v_2(3^{m_2}6^{n_2}))),$$

hence $v_3(3^{m_1}6^{n_1}) - v_2(v_3(3^{m_1}6^{n_1} = ((v_3(3^{m_2}6^{n_2}) - v_2(v_3(3^{m_2}6^{n_2})$ and $v_2(3^{m_1}6^{n_1}) = v_2(3^{m_2}6^{n_2})$. By definition of p-adic valuations on rational numbers, this is equivalent to $m_1 + n_1 - n_1 = m_2 + n_2 - n_2$ and $n_1 = n_2$ (as 3 appears in the prime factorization once for each power of 6 as well as for each power of 3). Hence $m_1 = m_2$ and $n_1 = n_2$. From this it follows that the preimages are the same, as by substitution we have $3^{m_1}6^{m_1} = 3^{m_2}6^{m_2}$.

To show that ϕ is bijective, we start by proving that it is injective. Consider two arbitrary elements a, b in G. By definition of G, $a = 3^{m_1}2^{n_1}$ and $b = 3^{m_2}2^{n_2}$, for integers m_1, n_1, m_2 and n_2. Suppose that $\phi(a) = \phi(b)$. Then $(v_3(a) - v_2(a), v_2(a)) = (v_3(b) - v_2(b), v_2(b))$. Hence $v_3(a) - v_2(a) = v_3(c) - v_2(b)$ and $v_2(a) = v_2(b)$. By definition of v_2 and v_3, and since factors of 2 appear for each n_1 and n_2 in 6, and once for each m_1 and m_2, it follows that $m_1 + n_1 - n_1 = m_1 = m_2 + n_2 - n_2 = m_2$, hence $m_1 = m_2$. Furthermore, $v_2(a) = v_2(b)$, so $n_1 = n_2$. So we have

$$a = 2^{n_1}3^{n_1+m_1} = 3^{m_1}6^{n_1} = 3^{m_2}6^{n_2} = b.$$

Since a, b are arbitrary, it follows that for all elements in G, $\phi(a) = \phi(b)$ implies that $a = b$. Hence ϕ is injective.

Let $y \in \mathbb{Z} \oplus \mathbb{Z}$ be an arbitrary element. Then $y = (m, n)$ for integers m and n. Clearly $x = 3^m 6^n$ is in G by definition of G. Then by definition of v_2 and v_3, $v_3(x) = m + n$, and $v_2(x) = n$. Then $\phi(3^m 6^n) = (m, n) = y$. Hence there is some element in G that maps to y under ϕ. Thus it follows that ϕ is injective.

Finally, to show that ϕ is operation preserving, consider arbitrary $a, b \in G$. Then by definition of G, $a = 3^{m_1}6^{n_2}$

$\boxed{\text{remark}}$ This argument does not hold for for $G = \{3^m 9^n : m, n \in \mathbb{Z}\}$, as $9 = 3^2$, hence any element in G could simply be written as $3^m 3^{2n} = 3^{2n+m}$. In this case, my ϕ function would always map to $(0, 2m + m)$, as $v_2(3^{2n+m}) = 0$ and $v_3(3^{2n+m}) = 2n + m$. Note that this does not mean that these are not isomorphic. It only means that my proof won't work in this case. I believe in fact that they are isomorphic.

$\boxed{\text{56: problem}}$ Suppose ϕ is an isomorophism from $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ to $\mathbb{Z}_{15}$, and $\phi(2,3) = 2$. Find the element in $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ that maps to 1.

$\boxed{\text{solution}}$ Note that in $\mathbb{Z}_{15}$ $8(2) = 1$. In other words, operating 2 with itself eight times is 1. Since $\phi((2,3)) = 2$, it follows that $8\phi((2,3)) = 1$. Since isomorphisms are operation preserving and by definition of an external direct product, we receive the following: $\phi(8(2,3)) = \phi((8(2), 8(3))) = \phi((1,4)) = 1$. Hence, $(1,4)$ is the element that is mapped to 1 by ϕ.

$\boxed{\text{70: question}}$ Without any calculations, how many subgroups of $U(27)$ are there.

$\boxed{\text{solution}}$ $27 = 3^3$, and 3 is an odd prime. So by a corollary to theorem 8.3 it follows that $U(27) \cong \mathbb{Z}_{3^3 - 3^2} = \mathbb{Z}_{18}$. Furthermore, $18 = 3^2 * 2$, hence the positive divisors of 18, the order of $\mathbb{Z}_{18}$, are $1, 2, 3, 6, 9, 18$, in total, there are 6 of them. By the fundamental theorem of finite cyclic groups (group of units mod n are always cyclic), it follows that there are in total six subgroups of $\mathbb{Z}_{18}$. Since $\mathbb{Z}_{18} \cong U(27)$ and subgroups are preserved under isomorphism, it follows that there are 6 subgroups of $U(27)$.

$\boxed{\text{6: proposition}}$ Let H and K be subgroups of G and let $HK = \{hk | h \in H, k \in K\}$ and $KH = \{kh | k \in K, h \in H\}$. Prove that HK is a group if and only if $HK = KH$.

$\boxed{\text{proof}}$ This proof will be shown in two parts. Let H, K, HK, KH and G be defined as instantiated above. Let us first suppose that HK is a group. Let a be an arbitrary element in HK. Then there exist some $h \in H, k \in K$ such that $a = hk$. By the inverse property of HK, it follows that $a^{-1} = (hk)^{-1} \in HK$. By the socks-shoe-property it follows that $(hk)^{-1} = k^{-1}h^{-1}$. Since H and K are groups themselves, we know that $h^{-1} \in H, k^{-1} \in K$. By definition of KH, it follows that $k^{-1}h^{-1} = (hk)^{-1} = a^{-1} \in KH$. Thus, for every element $a \in HK$ such that $a \in KH$ it follows that $HK \subseteq KH$.

Let furthermore b be an arbitrary element in KH. Since K and H are groups, there exists an inverse for every element $k \in K$ and $h \in H$. By construction of KH, let $b = k^{-1}h^{-1}$ for some $k^{-1} \in K, h^{-1} \in K$. By the socks-shoe-property it follows that $b = k^{-1}h^{-1} = (hk)^{-1}$. Since HK is a group, we know that $b = (hk)^{-1} \in HK$. Since b was chosen arbitrarily, it follows that $KH \subseteq HK$. Hence, by taking both parts together, $HK = KH$.

In order to show the other direction, let us suppose that $HK = KH$. Since $HK \subseteq G$, it suffices to show that $HK \leq G$. We will proceed by the two-step subgroup test. Let us first show the inverse property of HK. Let a be an arbitrary element in HK. Then there exist some elements $h \in H, k \in K$, such that $a = hk$. Consider $a^{-1} = (hk)^{-1}$. By the socks-shoes-property it follows that $(hk)^{-1} = k^{-1}h^{-1}$. Since $k^{-1}h^{-1} \in KH$ by definition of KH and inverse property of H and K, it follows that $a^{-1} = (hk)^{-1} \in HK$ as well because $HK = KH$. Furthermore, let $a = h_1k_1$ and $b = h_2k_2$ be arbitrary elements in HK. Consider $ab = h_1k_1h_2k_2 = h_1(k_1h_2)k_2$. By definition of KH we know that $k_1h_2 \in KH$. Since $KH = HK$, there exist some $k_3 \in K$ and $h_3 \in H$ such that $k_1h_2 = h_3k_3$. Thus, it follows that $h_1(k_1h_2)k_2 = h_1(h_3k_3)k_2 = (h_1h_3)(k_3k_2)$. Since $h_1h_3 \in H$ and $k_3k_2 \in K$ by the closure property of H and K, $ab \in HK$ and thus HK fulfills the closure property. Since HK fulfills the inverse and the closure property, it follows that $HK \leq G$ and thus HK is a group. qed.

$\boxed{\text{2: proposition}}$ Prove that A_n is normal in S_n.

$\boxed{\text{proof}}$ In order to show this, we will apply the Normal Subgroup Test. We already know that A_n forms a subgroup of S_n. Let x be an arbitrary element in S_n and y be an arbitrary element in xA_nx^{-1}. Thus, there exists some $y_1 \in A_n$ such that $y = xy_1x^{-1}$. Since $x \in S_n$, it can be expressed in two-cycles, the same is true for x^{-1}. Their number of two-cycles then have the same parity (consider the inverse property of A_n, for instance, which means that if x has an even number of two-cycles, then the same is true for x^{-1}). Since $y_1 \in A_n$, it has an even number of two-cycles. Putting this together, we know that $y = xy_1x^{-1}$ has an even number of two-cycles and thus $y \in A_n$. Hence, $xA_nx^{-1} \subseteq A_n$ and A_n is a normal subgroup of S_n. qed.

$\boxed{\text{7: proposition}}$ Let $G = GL(2, \mathbb{R})$ and let $K \leq \mathbb{R}*$. Prove that $H = \{A \in G | detA \in K\}$ is a normal subgroup of G.

$\boxed{\text{proof}}$ Let G, K and H be defined as stated above. We know that $H \subseteq G$, but we do not necessarily know yet that H forms a subgroup of G. Let us thus first show that. Consider the 2x2 identity matrix I with $det(I) = 1$. Since K forms a group, $1 \in K$ by the identity property. Thus it follows that $I \in H$, which implies that H is non-empty. Furthermore, let A, B be arbitrary elements in H. Consider $det(AB^{-1}) = det(A)det(B^{-1}) = det(A)/det(B) \in K$ by properties of closure and inverses of K. Hence, it follows that $AB^{-1} \in H$ and by the 1-step-subgroup-test $H \leq G$.

Now it remains to show that $XHX^{-1} \subseteq H$ for all $X \in G$. Let X be an arbitrary element in G and Y an arbitrary element in XHX^{-1}. Then there exists some $Y_1 \in H$ such that $Y = XY_1X^{-1}$. Consider $det(Y) = det(XY_1X^{-1}) = det(X)det(Y_1)det(X^{-1}) = det(X)det(Y_1)/det(X)$. Since determinants are real numbers, they commmute and we receive the following: $det(Y) = det(X)det(Y_1)/det(X) = det(Y_1)$. Since $Y_1 \in H$, we know that $det(Y) = det(Y_1) \in K$. This implies that $Y \in H$, considering that $Y \in G$ as well, since the dimension of the product remains unchanged when multiplying two square matrices of equal dimension. Since $XHX^{-1} \subseteq H$ and Y and X were chosen arbitrarily, it follows by the normal subgroup test that H is a normal subgroup of G. qed.