Abstract Algebra

August, Evelyn

10/19/2021

$\boxed{\text{6: question}}$ Let $n \in \mathbb{N}$, and let $H = \{mn : m \in \mathbb{Z}\}$. How many left cosets of H in Z are there?

$\boxed{\text{solutoin/proposition}}$ There are $n-1$ distinct left cosets of of H.

$\boxed{\text{proof}}$ Let H be instantiated as in the question. By the properties of cosets, we know that given an element $a \in \mathbb{Z}$, $a+H = H$ if and only if $a \in H$. By definition of H, this occurs only when there exists some $m \in \mathbb{Z}$ such that $a = mn$. In other words $a \equiv 0 \pmod{()n}$. Call the negation of this Condition 1). Furthermore, given arbitrary integers a and b, we have by another property of cosets that $a + H = b + H$ if and only if $a \in b + H$. By definition of H and of left cosets, this only occurs when there exists some $x \in \mathbb{Z}$ such that $a = b + xn$. Equivalently, this only happens when $a - b = xn$ for some $x \in \mathbb{Z}$, which means $n|a - b$, which also means that $a \equiv b \pmod{()n}$. Call the negation of this condition 2).

Let a be an arbitrary integer satisfying condition 1). Furthermore, we need to find the number of elements, b, satisfying condition 2). These will be elements which are not in the modular equivalence class of a modulo n. Since $[a]$ by assumption of condition 1) is not $[0]$, and neither is $[b]$, we have $n-2$ other options. Including $[a]$ into this we have in total $n-1$ options. Hence there are $n-1$ distinct left inverses of H. Q.E.D.

$\boxed{\text{12: proposition}}$ Given a group G such that $|G| = 155$, and elements $a, b \in G$ such that a and b are not the identity element, and $|a| \neq |b|$, it follows that any subgroup containing both a and b is itself G.

$\boxed{\text{proof}}$ Let G be instantiated as stated in the proposition, and let a, b be elements as stated in the proposition. Note that the prime factorization of 155 is $155 = 31 \cdot 5$. Hence the only positive divisors of 155 are $1, 5, 31$ and 155. By corollary 2 of Lagrange's theorem, the order of any subgroup divides the order of the group. Hence, given an arbitrary subgroup $H \leq G$, it follows that $|H| - 155, 31, 5$ or 1. Furthermore, since $| < a > | = |a|$ and $| < b > | = |b|$, and since a, b are not the identity element, there are only three options for the orders of a and b. Either $|a| = 31$ and $|b| = 5$, $|a| = 155$ and $|b| = 5$, or $|a| = 155$ and $|b| = 31$. (of course, we could interchange a with b for six more cases, but since a and b are arbitrary, we can narrow the cases down to these three). Suppose H contains both a and b. Then since the cyclic subgroups generated by a and b must by the closure property be subgroups of H, it follows by Corollary-2 that $|a|, |b|||H|$.
Hence in either of the last two cases, $155||H|$. But since $|H||155$, it follows that $|H| = 155 = |G|$, hence $H = G$. Suppose then that the first case is true, and that $|a| = 31$ and $|b| = 5$. Then $31, 5||H|$. Then by properties of division, it follows that since 31 and 5 are relatively prime, $155||H|$. Once again, taking into account that $|H||155$, it follows that $|H| = 155 = |G|$. Hence in this case also $H = G$.

Having shown that for all possible orders of a and b, $a, b \in H$ implies $H = G$, it follows for all non-identity elements $a, b \in G$ with different orders, if $a, b \in H$ then $H = G$.

$\boxed{\text{42: proposition}}$ Given a group G with order n, and an integer k relatively prime to n, the map $g \to g^k$ for all $g \in G$ is injective. Furthermore, if G is Abelian then this map is an automorphism on G.

$\boxed{\text{proof}}$ Let G be a group of order n and let k be a positive integer relatively prime to n. To show that the map $g \to g^k$ is injective, let g_1 and g_2 be arbitrary elements in G such that $g_1^k = g_2^l$.

By a theorem from chapter 4, we know that $|g_1^k| = |g_1|/\gcd(k, |g_1|)$ and $|g_2^k| = |g_2|/\gcd(k, |g_2|)$. Since $|g_1|$ is the order of the cyclic group generated by g_1, and likewise for g_2, By a corollary to Lagrange's theorem it follows that $|g_1|\big|n$ and $|g_2|\big|n$. Furthermore, since n and k are relatively prime, it follows that k is relatively prime to the orders of g_1 and g_2 as well. Hence $\gcd(k, |g_1|) = 1 = \gcd(k, |g_2|)$. Substituting in, we have $|g_1^k| = |g_1|$ and $|g_2^k| = |g_2|$. By supposition that $g_1^k = g_2^k$, it follows by substitution that $|g_1^k| = |g_2^k| = |g_1| = |g_2|$

Furthermore, as we have shown that $\gcd(|g_1|, k) = 1$ and $|g_2| = |g_1|$, it follows by Bezout's identity that $x|g_1| + yk = 1$ for integers x and y. Likewise, by substitution $1 = x|g_2| + yk$. So we have $g_1 = g_1^1 = g_1^{x|g_1|+yk} = (g_1^{|g_1|})^x g_1^{yk} = g_1^{yk} = (g_1^k)^y$. Likewise, for g_2, we have $g_2 = (g_2^k)^y$. By substitution, $g_1 = (g_1^k)^y = (g_2^k)^y = g_2$. Since g_1 and g_2 are arbitrary elements in G, it follows that for all $g_1, g_2 \in G$, $g_1^k = g_2^k$ implies $g_1 = g_2$. Hence the map $g \to g^k$ is injective.

$\boxed{\text{proof that this is an automorphism}}$ To show that the map $g \to g^k$ is an automorphism, we must show that it is surjective and operation preserving. To show that it is surjective, let h be an arbitrary element in G. By a corollary to Lagrange's theorem, $|h|\big|n$, since $|h| = |<h>| \leq G$. Hence $\gcd(|h|, k) = 1$, and by Bezout's identity it follows that $1 = x|h| + yk$ for integers x, y. Hence $h = h^1 = h^{x|h|+yk} = (h^{|h|})^x (h^y)^k = (h^y)^k$. Hence there exists some $g = h^y \in G$ such that $h = g^k$. Since h is arbitrary, it follows that for all $h \in G$ there exists some $g \in G$ such that $h = g^k$. Hence the codomain of the map $g \to g^k$ not only is of the same cardinality, but in fact is the domain. Hence the map $g \to g^k$ is surjective. Since it is injective as well, it follows that it is bijective.

It remains to be shown that $g \to g^k$ is operation preserving. To show this, let g_1 and g_2 be arbitrary elements in G. Then $g_1 g_2$ maps to $(g_1 g_2)^k$, which by associativity is equal to $g_1^k g_2^k$, if $k > 0$. If $k < 0$, $(g_1 g_2)^k$ is equal to $g_2^k g_1^k$ by associativity and the socks shoes property. However, if G is Abelian, it follows that $g_2^k g_1^k = g_1^k g_2^k$. Hence $g \to g^k$ is operation preserving. Thus, we have shown that the mapping is an automorphism.

$\boxed{\text{45: problem}}$ Let $G = \{(1), (12)(34), (1234)(56), (13)(24), (1432)(56), (56)(13), (14)(23), (24)(56)\}$

Find stab(1) and orb(1)

$stab(1) = \{(1), (24)(56)\}, orb(1) = \{1, 2, 3, 4\}$

Find stab(3) and orb(3)

$stab(3) = \{(1), (24)(56)\} = stab(1), orb(3) = \{1, 2, 3, 4\} = orb(3)$

Find stab(5) and orb(5)

$stab(5) = \{(1), (12)(34), (13)(24), (14)(23)\}, orb(5) = \{5, 6\}$

$\boxed{\text{48: proposition}}$ Let G be a group of order pqr (p, q and r are distinct primes). If H and K are subgroups of G with $|H| = pq \wedge |K| = qr$, prove that $|H \cap K| = q$.

$\boxed{\text{proof}}$ Let G, H and K be groups or subgroups as instantiated above. By problem 32 in Chapter 3 we know that $H \cap K$ forms a subgroup of G, and hence also of K and H. By Lagrange's Theorem, we know that the order of a subgroup divides the order of a finite group, which means that $|H \cap K|\,\big|\,|H|$ and $|H \cap K|\,\big|\,|K|$. Thus, the order of $H \cap K$ must divide both pq and qr. Since p, q and r are prime, it follows that $|H \cap K|$ either 1 or q. By Theorem 7.2 is follows that $|HK| = |H||K|/|H \cap K| = pq^2r$ or pqr. Since HK is a subset of G, the order of HK cannot be higher than $|G| = pqr$, hence it follows that $|H \cap K| = q$. QED.

$\boxed{\text{61: proposition}}$ Let $G = (2, \mathbb{R})$. Let H be the subgroup of matrices of determinant $+1$ or -1. If $a, b \in$ and $aH = bH$, what can be said about $\det(a)$ and $\det(b)$? Prove or disprove the converse.

$\boxed{\text{proof}}$ Let a, b be arbitrary elements in G s.t. $aH = bH$. By Lemma 4 in Chapter 7 it follows that $b \in aH$. This means that there exists some element $h \in H$ s.t. $b = ah$. Consider $\det(b) = \det(ah) = \det(a)\det(h) = |det(a)|$. Hence, $\det(b) = |\det(a)|$.

$\boxed{\text{proof of the converse}}$ Let a, b be arbitrary elements in G s.t. $\det(b) = |\det(a)|$. Consider $a^{-1}b$, which is in G by properties of closure and inverses. Then, it follows that $\det(a^{-1}b) = \det(a^{-1})\det(b) = \det(b)/\det(a^{-1}) = |1|$. By definition of H, it follows that $a^{-1}b \in H$, which, by a Lemma of cosets implies that $aH = bH$. Hence, $\det(b) = |\det(a)|$ iff $aH = bH$. QED.