Abstract Algebra

11_8
Samuel L. Peoples, CST, MA-C
November 8, 2016

30. Let r be a positive integer and let $\phi : \mathbb{R}^* \to \mathbb{R}^*$ be defined by $\phi(x) = x^r$. Do the following:

    (a) Show that ϕ is a homomorphism.

    Observe $\phi(ab) = (ab)^r = (ab)(ab)\ldots(rtimes) = a(rtimes) \cdot b(rtimes) = a^r b^r$
    Thus ϕ is a homomorphism.

    (b) Compute $\ker \phi$.

    Observe $e = 1$, thus $ker\phi = \{a \in \mathbb{R}^* \mid \phi(a) = 1\} = \{1\}$
    $1^r = 1$ for all $r \in \mathbb{R}$

    (c) Which values of r yield an isomorphism? Explain.

    Although ϕ is 1-1 for all r, for ϕ to be onto, where the output is $\mathbb{R}^*$, r=1.
    If $r > 1$, the output will be missing relatively prime values.

31. Let $\phi : G \to \overline{G}$ be a group homomorphism. Prove ϕ is one-to-one if and only if $\ker \phi = \{e\}$ where e is the identity of G.

    Proof.

    $\Rightarrow$ Suppose ϕ is 1-1. Recall $\phi(e) = \overline{e}$.

    Let $x \in ker\phi$. Observe $\phi(x) = \overline{e} = \phi(e)$($\phi$ 1-1, properties of ϕ)

    Therefore $ker\phi = \{e\}$

    $\Leftarrow$ Suppose $ker\phi = \{e\}$, Let $a, b \in G$ and $\phi(a) = \phi(b)$

    Observe $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(b)\phi(b^{-1}) = \overline{e}$

    Therefore $\phi(ab^{-1}) \in ker\phi$, $a = b$, and ϕ is $1 - 1$.

    Therefore ϕ is one-to-one if and only if $\ker \phi = \{e\}$ $\square$

32. Show that S_4 is not isomorphic to D_{12}.

    Observe that the only orders for which S_4 can take are $\{1, 2, 3, 4\}$.

    Because there are elements of order 12 (30 degree rotation, for example) in D_{12}, S_4 is not 1-1 when mapped to D_{12}. Element of order n must be of order n when mapped.

    Therefore, S_4 is not isomorphic to D_{12}.

This page intentionally left blank.

Abstract Algebra

11_29

Samuel L. Peoples, CST, MA-C

November 28, 2016

43. Find all distinct left cosets of $\{1, 11\}$ in $U(30)$.

    $U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$, thus there are four distinct left cosets.

    $\{1, 11\}$,$7 \cdot \{1, 11\} = \{7, 17\}$,$13 \cdot \{1, 11\} = \{13.23\}$, and $19\{1, 11\} = \{19, 29\}$

44. Suppose that K is a proper subgroup of H and H is a proper subgroup of G. If $|K| = 42$ and $|G| = 420$, what are the possible orders of H?

    $|K|$ divides $|H|$ (Lagrange's Theorem)

    $|H| = 42k, k > 1, k \in \mathbb{Z}$ (K is proper subgroup of H)

    Observe $42k$ divides 420, so k divides $\frac{420}{42} = 10$. (H proper subgroup of G)

    Thus, since $1 < k < 10$, $|H| = 2(42) = 84$ or $5(42) = 210$.

45. Let H and K be subgroups of a group G.

    (a) Prove $H \cap K$ is a subgroup of G.

    Proof.

    Let H, and K be subgroups of a group G.

    Observe $\forall a, b \in H, ab \in H \forall a, b \in K, ab \in K$; thus, $\forall a, b \in H \cap K, ab \in H \cap K$.(Closure)

    Observe that H and K are subgroups of G, and thus inherit associativity; notice $H \cap K$ is a subgroup of G, and is thus associative.

    Because H and K are subgroups of G $e \in H, e \in K$, thus $e \in H \cap K$.(Identity)

    Notice that because H and K are subgroups of G, they contain inverses such that $\forall a \in H, \forall a \in K, aa^{-1} = e$, thus $\forall a \in H \cap K, aa^{-1} = e$. (Inverses)

    Because $H \cap K$ is closed under the operation of G, contains an identity, and inverse for all elements, and is associative, $H \cap K$ is a subgroup of G. □

    (b) Is $H \cap K$ a subgroup of H? Briefly justify your answer.

    Because $H \cap K$ contains all the properties of H and is a group itself, $H \cap K$ is a subgroup of H

    (c) If $|H| = 12$ and $|K| = 35$, then find $|H \cap K|$.

    Because $H \cap K$ is a subgroup of G, and H and K are subgroups of G, $|H \cap K|$ divides the order of G.

    Observe that $|H|$ and $|K|$ divides the order of G.

    Thus $|H \cap K|$ must divide 12 and 35, with a GCD of 1.

    Thus $|H \cap K| = 1$

46. Let G be a group with $|G| = pq$, where p and q are prime. Prove that every proper subgroup of G is cyclic.

    Proof.

    Let G be a group with $|G| = pq$, where p and q are prime.

    By Lagrange's Theorem, the order of each proper subgroup is a divisor of pq, being p, q, and 1.

    Notice a subgroup of order 1 is trivially cyclic.

    Because the subgroups of order p and q are of prime orders, Lagrange's Theorem gives us that p and q are cyclic.

    Therefore, each proper subgroup of G is cyclic. □

Abstract Algebra

12_1
Samuel L. Peoples, CST, MA-C
December 1, 2016

55. Calculate the number of elements of order 2 in each of $\mathbb{Z}_{16}$, $\mathbb{Z}_8 \oplus \mathbb{Z}_2$, $\mathbb{Z}_4 \oplus \mathbb{Z}_4$, and $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Do the same for the elements of order 4.

	2	4
$\mathbb{Z}_{16}$	1	2
$\mathbb{Z}_8 \oplus \mathbb{Z}_2$	3	4
$\mathbb{Z}_4 \oplus \mathbb{Z}_4$	3	12
$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	7	8

56. Is $\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 \cong \mathbb{Z}_{60} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2$? Is $\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 \cong \mathbb{Z}_{15} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{12}$? Explain.

    Yes. Observe $\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{60} \oplus \mathbb{Z}_6 \cong \mathbb{Z}_{60} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2$.

    Yes. Observe $\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 \cong \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \cong\cong \mathbb{Z}_{15} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{12}$

57. Show that $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has seven subgroups of order 2.

    Notice elements of $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ are of the form (a, b, c).

    In $\mathbb{Z}_2$, $(a, b, c)^2 = (a + a, b + b, c + c) = e_{\mathbb{Z}_2}$

    Excluding the identity, there are seven elements of order two.

    $(0, 0, 0), (1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 0, 1), (0, 1, 1)$, and $(1, 1, 1)$

    Thus, for each $(a, b, c) \in \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, there exists a subgroup of order 2, $\{e, a\}$.

58. The group $S_3 \oplus \mathbb{Z}_2$ is isomorphic to one of the following groups: $\mathbb{Z}_{12}$, $\mathbb{Z}_6 \oplus \mathbb{Z}_2$, A_4, D_6. Determine which one by elimination.

    $|S_3 \oplus \mathbb{Z}_2| = 3! \cdot 2 = 12$

    Observe that no element of S_3 nor Z_2 has an element of order 12, where S_3 is at most 6. Thus, $S_3 \oplus \mathbb{Z}_2$ is not cyclic and we cannot include $\mathbb{Z}_{12}$.

    Notice that $\mathbb{Z}_6 \oplus \mathbb{Z}_2$ is abelian, because both $\mathbb{Z}_6$ and $\mathbb{Z}_2$ are abelian. S_3 is not abelian, and we cannot include $\mathbb{Z}_6 \oplus \mathbb{Z}_2$.

    From previous notes, we can recall that A_4 is the group of even permutations on four elements; we can also note that there is no element of order six. Thus we cannot include A_4.

    By elimination, and because it has elements of order $6, D_6$ is isomorphic to $S_3 \oplus \mathbb{Z}_2$.

59. Prove or disprove that $\mathbb{Z} \oplus \mathbb{Z}$ is a cyclic group.

    For sake of contradiction, suppose $\mathbb{Z} \oplus \mathbb{Z}$ is cyclic.

    Thus there must exists integers $m, n, a, b \in \mathbb{Z}$ such that:
    $(0, 1) = m \cdot (a, b)$ where $a = 0$
    $(1, 0) = n \cdot (a, b)$ where $b = 0$

    Thus $(a, b) = (0, 0)$, where $(0, 0)$ is not a generator for $\mathbb{Z} \oplus \mathbb{Z}$ #

    Therefore, because there is no generator for $\mathbb{Z} \oplus \mathbb{Z}$, the group is not cyclic.

Abstract Algebra

12_6
Samuel L. Peoples, CST, MA-C
December 5, 2016

47. In D_4, consider the subgroups $K = \{R_0, D\}$ and $L = \{R_0, D, D', R_{180}\}$. Show that K is a normal in L and L is normal in D_4, but K is not normal in D_4. From this example, we say that normality is not transitive.

    Notice K, L are subgroups of D_4 (Closure)
    For all $l \in L$ and $k \in K$, $(l \cdot k \cdot l^{-1}) \in K$ from the $Normal\ Subgroup\ Test$:
    R$_0 \cdot R_0 \cdot R_0 = R_0$ $\quad \in K$
    R$_0 \cdot D \cdot R_0 = D$ $\quad \in K$
    D$\cdot R_0 \cdot D = R_0$ $\quad \in K$
    D $\cdot D \cdot D = D$ $\quad \in K$
    D' $\cdot R_0 \cdot D' = R_0$ $\quad \in K$
    D' $\cdot D \cdot D' = D$ $\quad \in K$
    R$_{180} \cdot R_0 \cdot R_{180} = R_0$ $\quad \in K$
    R$_{180} \cdot D \cdot R_{180} = D$ $\quad \in K$
    Thus, K is normal in L; where $g \cdot K \cdot g^{-1} = K$.
    For normality of L in D_4, similarly from above, for all $d \in D_4$ and $l \in L$, $d \cdot l \cdot d^{-1} \in L$ from the $Normal\ Subgroup\ Test$.
    Notice, for $R_{90}, R_{90}^{-1} = R_{270} \in D_4$, and $D \in K$, $R_{90} \cdot D \cdot R_{270} = D'K$.
    Therefore K is *not* normal in D_4 and normality is not transitive.

48. (a) Let H be a subgroup of G. Prove that if $|G : H| = 2$, then H is normal in G.

    Proof.
    Let H be a subgroup of G where $|G : H| = 2$
    Observe that there are two distinct left cosets $\{H, aH\}$, where aH are all elements in G, but not H.
    Notice that, by the $Definition\ of\ Normality$, for some $x \in G$;
    where $x \in H$, $xH = H = Hx$ and is thus in G
    and $x \in aH$ $xH = aH = Hx$
    Thus, for all $x \in G$, $xH = Hx$
    Therefore H is normal in G. □

    (b) Prove that A_n is a normal subgroup of S_n.

    Proof.
    Recall that from a previous homework problem, A_n is a subgroup of S_n, where $|A_n| = \frac{n!}{2}$, and $|S_n| = n!$
    Thus, $|S_n : A_n| = \frac{|S_n|}{|A_n|} = 2$
    Recall from above, because $|S_n : A_n| = 2$, A_n is a normal subgroup of S_n. □

49. Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$ where $i^2 = j^2 = k^2 = -1$, $-i = (-1)i, 1^2 = (-1)^2 = 1$, $ij = -ji = k$, $jk = -kj = i$, and $ki = -ik = j$. Do the following:

    (a) Construct the Cayley table for G.

	-1	1	-i	i	-j	j	-k	k
-1	1	-1	i	-i	j	-j	k	-k
1	-1	1	-i	i	-j	j	-k	k
-i	i	-i	-1	1	k	-k	-j	j
i	-i	i	1	-1	-k	k	j	-j
-j	j	-j	-k	k	-1	1	i	-i
j	-j	j	k	-k	1	-1	-i	i
-k	k	-k	j	-j	-i	i	-1	1
k	-k	k	-j	j	i	-i	1	-1

(b) Show that $H = \{1, -1\}$ is a normal subgroup of G.

Observe that for all $x \in G$, $1 \cdot x = x$, and $-1 \cdot x = -x$
By the $Normal\ Subgroup\ Test$, $xHx^{-1} = \pm 1 \in H$
Thus, H is normal in G

(c) Construct the Cayley table for G/H.

	H	-i,i,-j,j,-k,k
H	H	-i,i,-j,j,-k,k
-i,i,-j,j,-k,k	-i,i,-j,j,-k,k	H

50. Prove that a factor group of an Abelian group is Abelian. That is, if G is an Abelian group and H is a normal subgroup of G, then G/H is Abelian.

Proof.

Recall a group G is abelian if $ab = ba$ for all $a, b \in G$

Suppose G is an Abelian group and H is a normal subgroup of G

Let $aH, bH \in G/H$, where $(aH)(bH) = (ab)H$ by the definition of a factor group.

Because G is abelian, $(ab)H = (ba)H = (bH)(aH)$

Thus, $(aH)(bH) = (bH)(aH)$

Therefore, G/H is abelian. $\square$

51. Let $\phi : G \to \overline{G}$ be a group homomorphism. Prove that the subgroup $\ker \phi$ is normal in G.

Proof.

Recall that the kernel of a group is a subgroup, where $\phi(\ker \phi) = e_H$

Let $g \in G$, and $h \in \ker \phi$

Observe that $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1})$
$= \phi(g)e_H\phi(g^{-1})$
$= \phi(g)\phi(g^{-1})$
$= \phi(g)\phi(g)^{-1}$
$= e_H$

Therefore, by the $Normal\ Subgroup\ Test$, $\ker \phi$ is normal in G. $\square$

Abstract Algebra

12_8
Samuel L. Peoples, CST, MA-C
December 7, 2016

52. Use the First Isomorphism Theorem to prove that $S_n/A_n \cong \mathbb{Z}_2$.

    Proof.

    Consider the homomorphism $\phi : S_n \to \mathbb{Z}_2$ defined by $\phi(\alpha) = (a, b)$

    Let $\alpha \in S_n$ be even.

    Observe that $\ker \phi = \{\alpha \in S_n \mid \phi(\alpha) = (e_{\mathbb{Z}_2}, x)\}$
    $= \{\alpha \in S_n \mid (a, b) = (e_{\mathbb{Z}_2}, x)\}$
    $= A_n$
    Because $|(a, b)| = 2$ and $|A_n| = 2$, and A_n is normal in S_n.

    Observe that $\phi(S_n) = \mathbb{Z}_2$

    Therefore, by the $First\ Isomorphism\ Theorem$, $S_n/A_n \cong \mathbb{Z}_2$.

    □

53. Suppose that k is a divisor of n. Prove that $\mathbb{Z}_n / < k > \cong \mathbb{Z}_k$.

    Proof.

    Cosider $\phi : \mathbb{Z}_n \to \mathbb{Z}_k$ defined by $\phi(x) = x \mod k$.

    Observe $ker \phi = \{a \in \mathbb{Z}_n \mid \phi(a) = 0\}$
    $= \{a \in \mathbb{Z}_n \mid x \mod k = 0\}$
    $= < k >$

    Notice $\phi(\mathbb{Z}) = \mathbb{Z}_k$, thus ϕ is onto.

    By the first Isomorphism Theorem $\mathbb{Z}_n / < k > \cong \mathbb{Z}_{\ltimes k}$. □

54. (a) Let G be a group and let $Z(G)$ be the center of G. Prove that if $G/Z(G)$ is cyclic, then G is Abelian.

    Proof.

    Recall the center of a group is always normal to the group; thus $Z(G)$ is a normal subgroup of G.

    Because $G/Z(G)$ is cyclic, let $G/Z(G) = < nZ >$; let $a, b \in G$, and $x, y \in \mathbb{Z}$

    For some $i, j \in \mathbb{Z}$, $a \in n^i Z, b \in n^j Z$

    Recall that the center commutes for all elements in the group.

    Observe $ab = (n^i x)(n^j y) = (n^i n^j)(xy) = (n^{i+j})(xy) = (n^{j+i})(yx) = (n^j y)(n^i x) = ba$

    Therefore, $\forall a, b \in G$, $ab = ba$, and G is abelian. □

    (b) Suppose that G is a non-Abelian group of order p^3, where p is a prime, and $Z(G) \neq \{e\}$. Prove that $|Z(G)| = p$.

    Proof.

    Because G is a non-abelian p group, $|Z(G)| = p$ or p^2

    Suppose $|Z(G)| = p^2$

    This implies that $G/Z(G)$ is cyclic with an order of p, and G is therefore abelian. #

    By contradiction, $|Z(G)| = p$. □

60. Let $G = \mathbb{Z}_4 \oplus \mathbb{Z}_4$, $H = \{(0,0),(2,0),(0,2),(2,2)\}$, and $K = < (1,2) >$.

(a) Is G/H isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$? Justify.

Observe G/H contains 4 elements
$H, (1,0)+H, (0,1)+H, (1,1)+H$ with three cosets of order 2.
By classification, G/H is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

(b) Is G/K isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$? Justify.

Observe G/K has elements of the form (a,a)
Notice K cosists of the elements $\{(0,0),(1,2),(2,0),(3,2)$
Thus $|(1,1)+K| = 4 \in G/K$
G/K is cyclic of order 4 and isomorphic to $\mathbb{Z}_4$