

Test 1 Solutions

If $G = \mathbb{C}, \mathbb{R}, \mathbb{Q}$ or \mathbb{Z} , assume that the group operation is addition. Let $\mathbb{C}^*, \mathbb{R}^*$ and \mathbb{Q}^* refer to complex numbers without 0, real numbers without 0 and rational numbers without 0, respectively. Let \mathbb{R}^+ and \mathbb{Q}^+ refer to positive real numbers and positive rational numbers, respectively. Assume that the group operation in these cases (the last five) is multiplication (\times).

1. True or false. Give reasons.

(a) In \mathbb{Z} , the function $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $\phi(n) = 6n$ is a homomorphism.

SOLUTION: True. $\phi(n+m) = 6(n+m) = 6n + 6m = \phi(n) + \phi(m)$, so ϕ is a homomorphism.

(b) In \mathbb{Z} , the function $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $\phi(n) = 3n$ is an isomorphism.

SOLUTION: False. Note that $\phi(n) = kn$ is a homomorphism for any $k \in \mathbb{Z}$. It is injective if $kn = 0 \Rightarrow n = 0$, which is true for any $k \neq 0$. In particular, it is true for $k = 3$. For ϕ to be surjective, there must be an integer, n , such that $kn = 1$. This is impossible except when $k = \pm 1$, so ϕ is not an isomorphism. Note that ϕ is an isomorphism between \mathbb{Z} and $\text{range}[\phi] = 3\mathbb{Z}$.

(c) In \mathbb{Z} , the function $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $\phi(n) = -n$ is an isomorphism.

SOLUTION: True. From the above solutions, we deduce that ϕ is an isomorphism. There are only two automorphisms on \mathbb{Z} , the identity ($k = 1$) and $\phi(n) = -n$.

(d) In \mathbb{Q}^* , the function $\phi : \mathbb{Q}^* \rightarrow \mathbb{Q}^*$ defined by $\phi(a) = 1/a$ is an isomorphism.

SOLUTION: True. $\phi(ab) = \frac{1}{ab} = \frac{1}{a} \times \frac{1}{b} = \phi(a) \times \phi(b)$.

(e) \mathbb{R} is isomorphic to \mathbb{R}^+ .

SOLUTION: True. Let $\phi(x) = e^x$. $\phi(x+y) = e^{x+y} = e^x \times e^y = \phi(x) \times \phi(y)$, so ϕ is a homomorphism. ϕ is clearly a bijection, since it has a (well-known) inverse: $\phi^{-1}(x) = \ln x$.

2. Let $G = \left\{ \begin{pmatrix} a & b \\ -7b & a \end{pmatrix} \mid a, b \in \mathbb{Q}, |a| + |b| > 0 \right\}$.

(a) Show that G , with matrix multiplication as the binary relation, is an Abelian group.

SOLUTION: If $\left\{ \begin{pmatrix} a & b \\ -7b & a \end{pmatrix} \right\} \in G$ and $\left\{ \begin{pmatrix} c & d \\ -7d & c \end{pmatrix} \right\} \in G$, then

$$\left\{ \begin{pmatrix} a & b \\ -7b & a \end{pmatrix} \right\} \times \left\{ \begin{pmatrix} c & d \\ -7d & c \end{pmatrix} \right\} = \left\{ \begin{pmatrix} ac - 7bd & ad + bc \\ -7(ad + bc) & ac - 7bd \end{pmatrix} \right\} \in G.$$

. Thus, G is closed under matrix multiplication. If $A = \left\{ \begin{pmatrix} a & b \\ -7b & a \end{pmatrix} \right\} \in G$, then the determinant of A is $a^2 + 7b^2$, which can only be zero when $a = b = 0$, which is not the case. Therefore, A^{-1} exists. In

fact, $A^{-1} = \left\{ \begin{pmatrix} \frac{a}{a^2+7b^2} & \frac{-b}{a^2+7b^2} \\ \frac{7b}{a^2+7b^2} & \frac{a}{a^2+7b^2} \end{pmatrix} \right\} \in G$. This makes G a subgroup of the group of invertible 2×2

matrices in $M(\mathbb{Q}_2)$.

Since $ac - 7bd = ca - 7db$ and $ad + bc = da + cb$, G is Abelian.

- (b) Let $G' = \{a + b\sqrt{-7} \mid a, b \in \mathbb{Q}, |a| + |b| > 0\}$. Show that G' , with multiplication as the binary relation, is isomorphic to G .

SOLUTION: $(a + b\sqrt{-7})(c + d\sqrt{-7}) = (ac - 7bd) + (ad + bc)\sqrt{-7} \in G'$, so $\phi : G' \rightarrow G$ defined by:

$$\phi(a + b\sqrt{-7}) = \left\{ \left(\begin{array}{cc} a & b \\ -7b & a \end{array} \right) \right\}$$

is a homomorphism. It is clearly injective and bijective. In general, numbers of the form $a + b\sqrt{d}$, where $a, b \in \mathbb{Q}$ and $\sqrt{d} \notin \mathbb{Q}$, form a group under multiplication that is isomorphic to an Abelian subgroup of invertible 2×2 matrices with rational coefficients.

- (c) Let $G_1 = \mathbb{Z} \pmod{5}$, with 0 removed. This is an Abelian group of order 4 under multiplication. Using trial and error, show that G_1 is cyclic.

SOLUTION: Try $a = 2$ as a generator. Then $\{a^0, a^1, a^2, a^3\} = \{2, 4, 3, 1\}$, so G_1 is cyclic.

- (d) Does $\sqrt{2}$ exist in G_1 ? That is, is there any $a \in G_1$ such that $a^2 = 2 \pmod{5}$?

SOLUTION: $1^2 = 4^2 = 1$ and $2^2 = 3^2 = 4$, so 2 (and 3) do not possess square roots. In \mathbb{Z}_p^* , the multiplicative group of non-zero integers \pmod{p} , where p is a prime, only half the elements have square roots. This is easy to observe, because the $p - 1$ elements of the group may be paired, k with $p - k$, for $k = 1, 2, \dots, \frac{p-1}{2}$. Observe that $k^2 = (p - k)^2 \pmod{p}$, so only half of the group elements can appear as squares of other elements.

- (e) Let $G_2 = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z} \pmod{5}, (a, b) \neq (0, 0)\}$. Show that G_2 is an Abelian group under "multiplication" defined by $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$. (All of this is $\pmod{5}$. That is, $7 - 11\sqrt{2} = 2 + 4\sqrt{2}$, for example.)

SOLUTION This problem can easily be recast in terms of 2×2 matrices whose elements are in \mathbb{Z}_5 . Multiplication is clearly commutative. Given the previous problems in this section, it is sufficient to show that if a or b is not 0, and if c or d is not 0, then either $ac + 2bd \neq 0$ or $ad + bc \neq 0$. Note first that $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$. This can only be 0 if both a and b are zero. Thus, if $(a + b\sqrt{2})(c + d\sqrt{2}) = 0$, then multiply by $(a - b\sqrt{2})(c - d\sqrt{2})$ to obtain $(a^2 - 2b^2)(c^2 - 2d^2) = 0$, forcing either $a^2 - 2b^2 = 0$ or $c^2 - 2d^2 = 0$.

Some examples. $(3 + \sqrt{2})(3 - \sqrt{2}) = 9 - 2 = 2 \pmod{5}$. The inverse of 2 is 3 and $3 - \sqrt{2} = 3 + 4\sqrt{2}$. This means that the inverse of $3 + \sqrt{2}$ is $3(3 + 4\sqrt{2}) = 4 + 2\sqrt{2} \pmod{5}$. Check as follows: $(3 + \sqrt{2})(4 + 2\sqrt{2}) = (12 + 4) + (6 + 4)\sqrt{2} = 1 \pmod{5}$.

- (f) What is $|G_2|$?

SOLUTION: $|G_2| = 24$. $|G_1| = 4$, so it is easy to make an error by setting $|G_2| = 4^2 = 16$. In fact, all of the 5^2 elements of $\mathbb{Z}_5 \times \mathbb{Z}_5$ are in G_2 , with the single exception of $(0, 0)$. The total is then $5^2 - 1$.

(g) Is G_2 cyclic?

SOLUTION: Yes it is, but I don't expect this to be obvious.

Try $g = 1 + \sqrt{2}$.

n	g^n
1	$1 + 1\sqrt{2}$
2	$3 + 2\sqrt{2}$
3	$2 + 0\sqrt{2}$
4	$2 + 2\sqrt{2}$
5	$1 + 4\sqrt{2}$
6	$4 + 0\sqrt{2}$
7	$4 + 4\sqrt{2}$
8	$2 + 3\sqrt{2}$
9	$3 + 0\sqrt{2}$
10	$3 + 3\sqrt{2}$
11	$4 + 1\sqrt{2}$
12	$1 + 0\sqrt{2}$

Try $g = 1 + 2\sqrt{2}$

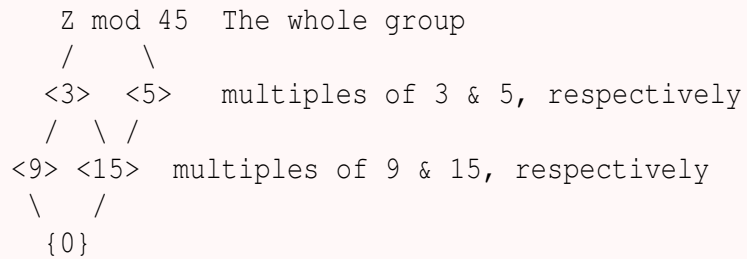
n	g^n
1	$1 + 2\sqrt{2}$
2	$4 + 4\sqrt{2}$
3	$0 + 2\sqrt{2}$
4	$3 + 2\sqrt{2}$
5	$1 + 3\sqrt{2}$
6	$3 + 0\sqrt{2}$
7	$3 + 1\sqrt{2}$
8	$2 + 2\sqrt{2}$
9	$0 + 1\sqrt{2}$
10	$4 + 1\sqrt{2}$
11	$3 + 4\sqrt{2}$
12	$4 + 0\sqrt{2}$
13	$4 + 3\sqrt{2}$
14	$1 + 1\sqrt{2}$
15	$0 + 3\sqrt{2}$
16	$2 + 3\sqrt{2}$
17	$4 + 2\sqrt{2}$
18	$2 + 0\sqrt{2}$
19	$2 + 4\sqrt{2}$
20	$3 + 3\sqrt{2}$
21	$0 + 4\sqrt{2}$
22	$1 + 4\sqrt{2}$
23	$2 + 1\sqrt{2}$
24	$1 + 0\sqrt{2}$

By trial and error, we see that $\langle 1 + 2\sqrt{2} \rangle = G_2$.

3. (a) Compute $(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}) / \langle (2,3) \rangle$. Note that $\langle (2,3) \rangle$ is the cyclic subgroup generated by $(2,3)$.
 SOLUTION: To compute a factor group, G/H , we need to know what H is. $(2,3)$ generates a cyclic subgroup, H , of order 10. The reason is that $\gcd(5,2) = 1$, so all of $\{0,1,2,3,4\}$ occur when $(2,3)$ is added to itself 5 times. But $5 \times (2,3) = (0,1)$, so it takes another 5 times to arrive at $(0,0)$. Thus $H = \{(a,b) \in \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \mid a \in \mathbb{Z}/5\mathbb{Z}, b \in \{0,3\}\}$. The cosets of H comprise the factor group, which has $30/10 = 3$ elements. Thus, the factor group is: $\{H, (0,1) + H, (0,2) + H\}$. It is isomorphic to \mathbb{Z}_3 , but not equal to \mathbb{Z}_3 .
- (b) What is the number of subgroups of $\mathbb{Z}/45\mathbb{Z}$?
 SOLUTION: There is a subgroup, H_n , of $G = \mathbb{Z}/45\mathbb{Z}$, for every integer, n , that divides 45. The divisors of 45 are 1, 3, 5, 9, 15 and 45. This yields 6 subgroups, of which 4 are proper and non-trivial.

- (c) Compute all the subgroups of $\mathbb{Z}/45\mathbb{Z}$ and draw a subgroup diagram as well.

SOLUTION:



- (d) Let p_1, p_2 and p_3 be three distinct prime numbers. How many distinct Abelian groups are there of order $p_1 p_2^2 p_3^3$ (up to isomorphism)?

SOLUTION: Because of the isomorphism theorem classifying finite(ly generated) Abelian groups, we know that any such group isomorphic to a finite product of factor groups of the form \mathbb{Z}_{p^k} , where p is a prime and k is a positive integer. Let's consider the three given primes, p_1, p_2 and p_3 . p_1 must occur. p_2 can occur in two ways as $\mathbb{Z}_{p_2^2}$ or as $\mathbb{Z}_{p_2} \times \mathbb{Z}_{p_2}$. p_3 can occur in three ways as $\mathbb{Z}_{p_3^3}$, as $\mathbb{Z}_{p_3} \times \mathbb{Z}_{p_3^2}$, or as $\mathbb{Z}_{p_3} \times \mathbb{Z}_{p_3} \times \mathbb{Z}_{p_3}$. There are $2 \times 3 = 6$ choices, and therefore 6 different groups, up to isomorphism.

- (e) Let $G = \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$. Compute all the subgroups of G .

SOLUTION: Let $g_1 = (1, 0, 0, 0)$, $g_2 = (0, 1, 0, 0)$, $g_3 = (0, 0, 1, 0)$ and $g_4 = (0, 0, 0, 1)$. Any $g \in G$ can be written as $g = a \cdot g_1 + b \cdot g_2 + c \cdot g_3 + d \cdot g_4$, where $a \in \mathbb{Z}/11\mathbb{Z}$, $b \in \mathbb{Z}/25\mathbb{Z}$, $c \in \mathbb{Z}/3\mathbb{Z}$ and $d \in \mathbb{Z}/9\mathbb{Z}$. Classifying all $H \leq G$ is equivalent to describing all possible generators for H . Taking $0 \cdot g_1$ or $1 \cdot g_1$ gives two possibilities. Taking $0 \cdot g_2, 5 \cdot g_2$ or $1 \cdot g_2$ gives three possibilities for each of the preceding two. However, not all subgroups of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ are cyclic. It turns out that there are ten subgroups of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$, rather than just six. The cyclic subgroups are: $\{0\}$, $\langle g_3 \rangle$, $\langle 3 \cdot g_4 \rangle$, $\langle g_4 \rangle$, $\langle g_3 + 3 \cdot g_4 \rangle$, $\langle g_3 + g_4 \rangle$, $\langle 2 \cdot g_3 + 3 \cdot g_4 \rangle$ and $\langle 2 \cdot g_3 + g_4 \rangle$. There remain two more non-cyclic subgroups generated by: $\{g_3, 3 \cdot g_4\}$, $\{g_3, g_4\}$.

Putting everything together, there are $2 \times 3 \times 10 = 60$ subgroups of G , including $\{0\}$ and G .

- (f) Give an example of a finite Abelian group, G , that has a subgroup, H such that H is isomorphic to G/H .

SOLUTION: It is clear that if $|H| = n$, then $G = |G/H| \times |H| = n^2$. $G_1 = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and $G_2 = \mathbb{Z}/n^2\mathbb{Z}$ are two possibilities for G . For G_1 , $H = \langle n \rangle$. For G_2 , $H = \langle (1, 0) \rangle$ or $H = \langle (0, 1) \rangle$ both work.

4. $15\mathbb{Z}$, $21\mathbb{Z}$ and $35\mathbb{Z}$ are three different subgroups of \mathbb{Z} . Compute the smallest subgroup of \mathbb{Z} that contains these three subgroups.

SOLUTION: If H contains all three subgroups, then $15 \in H$ and $21 \in H$. Since $\gcd(15, 21) = 3$, there are integers a and b such that $15a + 21b = 3$. ($3 \times 15 - 2 \times 21 = 3$). Thus, $3 \in H$. Since $\gcd(3, 35) = 1$, there are integers a and b such that $3a + 35b = 1$. ($3 \times 12 - 1 \times 35 = 1$). Thus, $1 \in H$, so $H = \mathbb{Z}$.

5. There are two types of “perfect” shuffles of a deck of (52) cards. a) Split the deck into two equal halves (26+26). Shuffle so that the bottom card in the shuffled deck is 26, the one on top of it is 52, the next is 25, and so on. The top card in the shuffled deck is 27. b) The deck is split the same way, but this time the bottom card is 52, the one on top of it is 26 and so on. The top card is 1. These shuffles generate permutations π_1 and π_2 of the deck, respectively.

- (a) How many orbits are there in π_1 ? How many shuffles does it take for the deck to return to its original order?

SOLUTION: It is easy to derive $\pi_1(n) = 2n$ if $n \leq 26$ and $\pi_1(n) = 2(n - 26) - 1$ if $n > 26$. Working by hand:

(1, 2, 4, 8, 16, 32, 11, 22, 44, 35, 17, 34, 15, 30, 7, 14, 28,
3, 6, 12, 24, 48, 43, 33, 13, 26, 52, 51, 49, 45, 37, 21, 42, 31, 9,
18, 36, 19, 38, 23, 46, 39, 25, 50, 47, 41, 29, 5, 10, 20, 40, 27)

There is one orbit. The permutation is a single cycle of order 52. It takes 52 shuffles to bring the deck back to its original order.

- (b) Same question as above for π_2 .

SOLUTION: It is easy to derive $\pi_2(n) = 2n - 1$ if $n \leq 26$ and $\pi_2(n) = 2(n - 26)$ if $n > 26$. Note that both 1 and 52 are fixed. Working by hand:

(1)
(2, 3, 5, 9, 17, 33, 14, 27)
(4, 7, 13, 25, 49, 46, 40, 28)
(6, 11, 21, 41, 30, 8, 15, 29)
(10, 19, 37, 22, 43, 34, 16, 31)
(12, 23, 45, 38, 24, 47, 42, 32)
(18, 35)
(20, 39, 26, 51, 50, 48, 44, 36)
(52)

There are nine orbits. The cycle decomposition contains 2 cycles of length 1, 1 cycle of length 2, and 6 cycles of length 8. The deck returns to its original order after 8 shuffles.

The shuffle $\pi_2\pi_1$ has a cycle decomposition of:

(1, 3, 11, 43, 14, 4, 15, 8, 31, 17, 16, 12, 47, 30, 13, 51, 46, 26,
52, 50, 42, 10, 39, 49, 38, 45, 22, 36, 37, 41, 6, 23, 40, 2, 7, 27)
(5, 19, 24, 44, 18, 20, 28)
(9, 35, 33, 25, 48, 34, 29)
(21, 32)

There are 4 orbits. The cycle decomposition has 1 cycle of size 36, 2 cycles of size 7, and a single cycle of size 2. The compound shuffle repeats every $36 \times 7 = 252$ times.