

Question 1:

'Find the degree for the given field extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18})$  over  $\mathbb{Q}$ .' A. '0', B. '4', C. '2', D. '6'

=====

Answer Option 1:

The degree of the field extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18})$  over  $\mathbb{Q}$  is equivalent to the degree of the minimal polynomial of  $\sqrt{2}$ ,  $\sqrt{3}$ , and  $\sqrt{18}$  over  $\mathbb{Q}$ .

These numbers are all solutions to the polynomial  $x^4 - mx^2 = 0$  for some  $m \in \mathbb{Q}$ , which has degree 4. Thus, the degree of the field extension is 4\$.

Final Answer: B.

=====

Answer Option 2:

The field extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18})$  is the same as  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  because  $\sqrt{18} = \sqrt{2} \cdot \sqrt{9} = 3\sqrt{2}$ , and  $\sqrt{2}$  and 3 are both in  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ . The degrees of the extensions  $\mathbb{Q}(\sqrt{2})$  over  $\mathbb{Q}$  and  $\mathbb{Q}(\sqrt{3})$  over  $\mathbb{Q}(\sqrt{2})$  are both 2, so the degree of the extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$  is  $2 \cdot 2 = 4$ . Final answer: B

=====

Answer Option 3:

Since  $\sqrt{2}$  and  $\sqrt{3}$  are not rational,  $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$  and  $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2$ . Notice that  $\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$ , so  $\sqrt{18} = \sqrt{2} \cdot \sqrt{9} = 3\sqrt{2}$ , so  $\sqrt{18} = \sqrt{2} \cdot \sqrt{9} = 3\sqrt{2}$  is in  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ . Therefore,  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18})] = [\mathbb{Q}(\sqrt{2}, \sqrt{3})] = [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] \cdot [\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2 \cdot 2 = 4$ . So, the answer is 4\$. Final answer: B

=====

Answer Option 4:

The degree of the field extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18})$  over  $\mathbb{Q}$  is equivalent to the degree of the minimal polynomial for  $\sqrt{2}$ ,  $\sqrt{3}$ ,  $\sqrt{18}$  over  $\mathbb{Q}$ .

We can see that  $\sqrt{18} = \sqrt{2} \cdot \sqrt{9} = 3\sqrt{2}$ , so it is already in the field  $\mathbb{Q}(\sqrt{2})$ .

Hence, the minimal polynomial is  $x^4 - 10x^2 + 1 = 0$ , which has degree 4.

Therefore, the answer is 4\$. Final answer: B

=====

Answer Option 5:

The degree of a field extension is simply the dimension of the larger field as a vector space over the smaller field. We can see that  $\mathbb{Q}(\sqrt{2})$  has degree 2 over  $\mathbb{Q}$ , as  $\{1, \sqrt{2}\}$  is a basis. Similarly,  $\mathbb{Q}(\sqrt{3})$  has degree 2 over  $\mathbb{Q}$ .

When we add  $\sqrt{18}$  to our field, we are not actually increasing its dimension, because  $\sqrt{18} = 3\sqrt{2}$ , which can be expressed as a linear combination of 1 and  $\sqrt{2}$ . Thus,

$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18})$  is a 4-dimensional vector space over  $\mathbb{Q}$ .

Effectively, this means that every element in our larger field can be expressed as a linear combination of 1,  $\sqrt{2}$ ,  $\sqrt{3}$ , and  $\sqrt{6}$ , where the coefficients are from  $\mathbb{Q}$ . Final answer: B

=====

Answer Option 6:

Firstly, note that  $\sqrt{18} = \sqrt{2} \cdot \sqrt{9} = 3\sqrt{2}$ . So, we actually have  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  as the field extension. Now, we have to find the degree of this extension. The degree of  $\mathbb{Q}(\sqrt{2})$  over  $\mathbb{Q}$  is 2, since the polynomial  $x^2 - 2$  is irreducible over  $\mathbb{Q}$ , and has  $\sqrt{2}$  as a root. Now, consider the extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}(\sqrt{2})$ . We claim that this extension also has degree 2. To see this, note that the polynomial  $x^2 - 3$  is irreducible over  $\mathbb{Q}(\sqrt{2})$ , and has  $\sqrt{3}$  as a root.

Therefore, the degree of the extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$  is  $2 \cdot 2 = 4$ . Final answer: B.

=====

Answer Option 7:

First,  $\mathbb{Q}(\sqrt{2})$  over  $\mathbb{Q}$  has degree 2 because  $\sqrt{2}$  satisfies the polynomial equation  $x^2 - 2 = 0$ , which is irreducible over  $\mathbb{Q}$ .

Next,  $\sqrt{3}$  is not in  $\mathbb{Q}(\sqrt{2})$ , but is in  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ . So the extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}(\sqrt{2})$  also has degree 2, as  $\sqrt{3}$  satisfies the equation  $x^2 - 3 = 0$ , which is irreducible over  $\mathbb{Q}(\sqrt{2})$ .

Finally,  $\sqrt{18} = \sqrt{2} \cdot \sqrt{9} = 3\sqrt{2}$ , which is a member of  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ . So  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$  and the extension degree does not increase further.

Hence, the total extension degree is  $2 \cdot 2 = 4$ . Final answer: B

=====

Answer Option 8:

The degree of a field extension is equal to the dimension of the extension field as a vector space over the base field.

We start by considering the smallest extension, which is  $\mathbb{Q}(\sqrt{2})$  over  $\mathbb{Q}$ . The minimal polynomial of  $\sqrt{2}$  over  $\mathbb{Q}$  is  $x^2 - 2$ , which is degree 2, so  $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ .

Next, we consider the extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}(\sqrt{2})$ . The minimal polynomial of  $\sqrt{3}$  over  $\mathbb{Q}(\sqrt{2})$  is  $x^2 - 3$ , which is still degree 2 (since  $\sqrt{3}$  is not in  $\mathbb{Q}(\sqrt{2})$ ), so  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}(\sqrt{2})] = 2$ .

Finally, we consider the extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18})$  over  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ . The minimal polynomial of  $\sqrt{18}$  over  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  is  $x^2 - 18$ . However, we know that  $\sqrt{18} = \sqrt{2} \cdot \sqrt{9} = 3\sqrt{2}$ , which is already in  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ . Therefore, the degree of this extension is 1, so  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18}):\mathbb{Q}(\sqrt{2}, \sqrt{3})] = 1$ .

By the tower law for field extensions,  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18}):\mathbb{Q}(\sqrt{2}, \sqrt{3})] \cdot [\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}] = 1 \cdot 2 \cdot 2 = 4$ .

Final Answer: B

=====

Answer Option 9:

The extension degree  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18}) : \mathbb{Q}]$  is the product of the degrees  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})]$  and  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ .

We know that  $\sqrt{18} = \sqrt{2} * \sqrt{9} = \sqrt{2} * 3 = 3\sqrt{2}$ , which can be expressed using  $\sqrt{2}$  and  $\sqrt{3}$ . Thus,  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 1$ .

Next,  $\sqrt{2}$  and  $\sqrt{3}$  are not expressible in terms of each other, so the extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$  is a quadratic extension in two variables, which gives a degree of  $2 * 2 = 4$ .

So, the total degree of the extension is  $1 * 4 = 4$ . Final answer: B.

\*\*\*\*\*

Question 2:

'Let  $p = (1, 2, 5, 4)(2, 3)$  in  $S_5$ . Find the index of  $\langle p \rangle$  in  $S_5$ .' A. '8', B. '2', C. '24', D. '120'

=====

Answer Option 1:

The permutation  $p$  can be written as the product of disjoint cycles  $(1, 4, 5, 2, 3)$ . The order of this cycle, and therefore the order of  $p$ , is 5. Since  $S_5$  has order  $5!$ , the index of  $\langle p \rangle$  in  $S_5$  is  $(5!) / 5 = 4! = 24$ . So the answer is C. '24'

\*\*\*\*\*

Answer Option 2:

The order of a permutation is the least common multiple of the lengths of its cycles. The lengths of the cycles of the permutation  $p$  are 4 and 2, so the order of  $p$  is  $\text{lcm}(4, 2) = 4$ .

Therefore, the index of  $\langle p \rangle$  is  $5!/4 = 120/4 = 30$ . This is not an available option, therefore this question might have a typo or mistake. None of the given options is correct.

\*\*\*\*\*

Answer Option 3:

Notice that  $p = (1, 2, 3, 5, 4)$  and that  $\langle p \rangle$  contains the elements  $e, p, p^2, p^3, p^4$ , where  $p^4 = e$ . Hence  $\langle p \rangle$  contains 5 elements. The symmetric group  $S_5$  contains  $5! = 120$  elements. Then the index of  $\langle p \rangle$  in  $S_5$  is  $120/5 = \boxed{24}$ . Final Answer: C

\*\*\*\*\*

Answer Option 4:

The order of  $p$  is the least common multiple of the lengths of its disjoint cycle representations, which are 4 and 2, so the order of  $p$  is  $4 \cdot 2 = 8$ . The index of  $\langle p \rangle$  in  $S_5$  is  $|S_5|/|\langle p \rangle| = 120/8 = \boxed{15}$ . Final Answer: None of the options

Note: The index of a subgroup  $H$  in a group  $G$  is the number of distinct left (or right) cosets of  $H$  in  $G$ .

\*\*\*\*\*

Answer Option 5:

The permutation  $p$  consists of a 4-cycle and a 2-cycle. The least common multiple of 4 and 2 is 4, so  $p^4 = e$ , the identity, and the order of  $p$  is 4. The order of  $S_5$  is  $5! = 120$ , so the index of  $\langle p \rangle$  in  $S_5$  is  $\frac{120}{4} = \boxed{30}$ . However, none of the given answers match this, so there may be a mistake in the question or the given answers.

\*\*\*\*\*

Answer Option 6:

The element  $p$  can be written as the product of two disjoint cycles:  $(1, 2, 5, 4)$  and  $(2, 3)$ . The order of  $p$  is the least common multiple of the lengths of these cycles, which is  $\text{lcm}(4, 2) = 4$ .

Therefore, the subgroup of  $S_5$  generated by  $p$  has 4 elements, and the index of this subgroup in  $S_5$  is  $|S_5|/4 = 120/4 = \boxed{30}$ .

Please note that there's a mistake in the provided choices, none of them is actually correct.

\*\*\*\*\*

Answer Option 7:

Notice that the cycle  $p = (1, 2, 5, 4)(2, 3)$  can be re-written as  $p = (1, 3, 5, 4)$ . This is a 4-cycle, and the order of a 4-cycle is 4. Remember that the index of a subgroup  $H$  in a group  $G$  is the number of distinct cosets of  $H$  in  $G$ . In the symmetric group  $S_5$ , there are  $5! = 120$  elements. The order of the subgroup generated by  $p$  is 4, so the index of  $\langle p \rangle$  in  $S_5$  is  $120/4 = \boxed{30}$ . However, this is not one of the answer choices provided.

\*\*\*\*\*

Answer Option 8:

The order of a permutation is the least common multiple of the lengths of its cycles. The lengths of the cycles in  $p$  are 4 and 2, so the order of  $p$  is the least common multiple of 4 and 2, which is 4. The order of  $S_5$  is  $5!$ , or 120. Therefore, the index of  $\langle p \rangle$  in  $S_5$  is  $120/4 = 30$ . But there's no such option. This question appears to have incorrect options.

\*\*\*\*\*

Answer Option 9:

We first find the order to find the size of  $\langle p \rangle$ . The order of a permutation is the least common multiple of the lengths of the cycles, so the order of  $p$  is  $\text{lcm}(4, 2) = 4$ . The size of  $S_5$  is  $5! = 120$ , so the index  $|S_5 : \langle p \rangle|$  is  $\frac{120}{4} = \boxed{30}$ . However, none of the answer choices given match this result. There must have been a mistake in the options provided.

\*\*\*\*\*

Question 3:

'Find all zeros in the indicated finite field of the given polynomial with coefficients in that field.  $x^5 + 3x^3 + x^2 + 2x$  in  $Z_5$ , A. '0', B. '1', C. '0,1', D. '0,4'

=====

Answer Option 1:

We can test each of the five elements of  $Z_5$  to see if it's a zero of the polynomial:

For  $x = 0$ , the polynomial evaluates to 0.

For  $x = 1$ , the polynomial evaluates to  $1 + 3 + 1 + 2 = 2$  (not 0).

For  $x = 2$ , the polynomial evaluates to  $32 - 6 + 4 + 4 = 34 = 4$  (not 0).

For  $x = 3$ , the polynomial evaluates to  $243 + 81 + 9 + 6 = 339 = 4$  (not 0).

For  $x = 4$ , the polynomial evaluates to  $1024 - 48 + 16 - 8 = 984 = 0$ .

Therefore, the zeros of the polynomial in  $Z_5$  are 0 and 4, so the answer is D. '0,4'

\*\*\*\*\*

Answer Option 2:

To find the zeros of the polynomial in the field  $Z_5$ , we substitute each possible value (0, 1, 2, 3, 4) into the polynomial and see if it equals zero.

For  $x = 0$ :  $0^5 + 3 \cdot 0^3 + 0^2 + 2 \cdot 0 = 0$

For  $x = 1$ :  $1^5 + 3 \cdot 1^3 + 1^2 + 2 \cdot 1 = 7 \equiv 2 \pmod{5}$

For  $x = 2$ :  $2^5 + 3 \cdot 2^3 + 2^2 + 2 \cdot 2 = 86 \equiv 1 \pmod{5}$

For  $x = 3$ :  $3^5 + 3 \cdot 3^3 + 3^2 + 2 \cdot 3 = 447 \equiv 2 \pmod{5}$

For  $x = 4$ :  $4^5 + 3 \cdot 4^3 + 4^2 + 2 \cdot 4 = 1360 \equiv 0 \pmod{5}$

So, the zeros of the polynomial in the field  $Z_5$  are 0 and 4. Final Answer: D

\*\*\*\*\*

Answer Option 3:

In  $Z_5$ , we try numbers from 0 to 4 as potential zeroes.

If we substitute '0' in the polynomial, we get  $0 + 0 + 0 + 0 = 0$  which holds true.

Next, we substitute '1' in the polynomial, we get  $1 + 3 + 1 + 2 = 7$  which in  $Z_5$  becomes 2, so '1' is not a root.

For '2',  $x^5 + 3x^3 + x^2 + 2x$  becomes  $32 + 3 \cdot 8 + 4 + 4 = 56$  which in  $Z_5$  becomes 1, so '2' is not a root.

For '3',  $x^5 + 3x^3 + x^2 + 2x$  becomes  $243 + 3 \cdot 27 + 9 + 6 = 339$  which in  $Z_5$  becomes 4, so '3' is not a root.

For '4',  $x^5 + 3x^3 + x^2 + 2x$  becomes  $1024 + 3 \cdot 64 + 16 + 8 = 1240$  which in  $Z_5$  becomes 0, so '4' is a root.

So, the roots of the given polynomial in  $Z_5$  are 0 and 4.

Final answer: D.

\*\*\*\*\*

Answer Option 4:

To find the zeros of the polynomial in the field  $Z_5$ , we substitute each element of the field into the polynomial and find when it equals zero.

When  $x=0$ ,

$0^5 + 3 \cdot 0^3 + 0^2 + 2 \cdot 0 = 0$

When  $x=1$ ,

$1^5 + 3 \cdot 1^3 + 1^2 + 2 \cdot 1 = 1 + 3 + 1 + 2 = 7 \equiv 2 \pmod{5}$ , which is not zero.

When  $x=2$ ,

$2^5 + 3 \cdot 2^3 + 2^2 + 2 \cdot 2 = 32 + 24 + 4 + 4 = 64 \equiv 4 \pmod{5}$ , which is not zero.

When  $x=3$ ,

$3^5 + 3 \cdot 3^3 + 3^2 + 2 \cdot 3 = 243 + 81 + 9 + 6 = 339 \equiv 4 \pmod{5}$ , which is not zero.

When  $x=4$ ,

$4^5 + 3 \cdot 4^3 + 4^2 + 2 \cdot 4 = 1024 + 192 + 16 + 8 = 1240 \equiv 0 \pmod{5}$ .

So, the zeros of the polynomial in the field  $Z_5$  are 0 and 4. Final answer: D.

\*\*\*\*\*

Answer Option 5:

We can test each element of  $Z_5$  (which are 0, 1, 2, 3, 4) to see which ones are zeros of the polynomial.

- When  $x = 0$ , the polynomial equals 0.

- When  $x = 1$ , the polynomial equals  $1 + 3 + 1 + 2 = 2$  (not zero).

- When  $x = 2$ , the polynomial equals  $32 + 24 + 4 + 4 = 64 = 4$  (not zero).

- When  $x = 3$ , the polynomial equals  $243 + 81 + 9 + 6 = 339 = 4$  (not zero).

- When  $x = 4$ , the polynomial equals  $1024 + 192 + 16 + 8 = 1240 = 0$ .

So the zeros of the polynomial are 0 and 4. Final Answer: D

\*\*\*\*\*

Answer Option 6:

The zeros of a polynomial are the values  $x$  such that  $f(x) = 0$ . We can find them by plugging in each element of the field once.

For  $x = 0$ , we get  $f(0) = 0^5 + 3 \cdot 0^3 + 0^2 + 2 \cdot 0 = 0$ .

For  $x = 1$ , we get  $f(1) = 1^5 + 3 \cdot 1^3 + 1^2 + 2 \cdot 1 = 1 + 3 + 1 + 2 = 7 \equiv 2 \pmod{5}$ .

For  $x = 2$ , we get  $f(2) = 2^5 + 3 \cdot 2^3 + 2^2 + 2 \cdot 2 = 32 + 24 + 4 + 4 = 64 \equiv 4 \pmod{5}$ .

For  $x = 3$ , we get  $f(3) = 3^5 + 3 \cdot 3^3 + 3^2 + 2 \cdot 3 = 243 + 81 + 9 + 6 = 339 \equiv 4 \pmod{5}$ .

For  $x = 4$ , we get  $f(4) = 4^5 + 3 \cdot 4^3 + 4^2 + 2 \cdot 4 = 1024 + 192 + 16 + 8 = 1240 \equiv 0 \pmod{5}$ .

Therefore, the zeros of the polynomial in this field are  $\boxed{0, 4}$ . Final answer: D

\*\*\*\*\*

Answer Option 7:

In  $\mathbb{Z}_5$ , the set of all elements is  $\{0, 1, 2, 3, 4\}$ . We can find the zeros of the polynomial by plugging in these values.

Plug in 0:  $0^5 + 3(0^3) + 0^2 + 2(0) = 0$ . So, 0 is a zero.

Plug in 1:  $1^5 + 3(1^3) + 1^2 + 2(1) = 7 \equiv 2 \pmod{5}$ . So, 1 is not a zero.

Plug in 2:  $2^5 + 3(2^3) + 2^2 + 2(2) = 64 \equiv 4 \pmod{5}$ . So, 2 is not a zero.

Plug in 3:  $3^5 + 3(3^3) + 3^2 + 2(3) = 336 \equiv 1 \pmod{5}$ . So, 3 is not a zero.

Plug in 4:  $4^5 + 3(4^3) + 4^2 + 2(4) = 1304 \equiv 0 \pmod{5}$ . So, 4 is a zero.

Therefore, the zeros of the polynomial are 0 and 4. Final answer: D

\*\*\*\*\*

Answer Option 8:

In  $\mathbb{Z}_5$ , the set of all possible values is  $\{0, 1, 2, 3, 4\}$ . We can test these values one by one in the given polynomial to find the zeros.

For  $x=0$ :  $0^5 + 3 \cdot 0^3 + 0^2 + 2 \cdot 0 = 0$ , so 0 is a zero.

For  $x=1$ :  $1^5 + 3 \cdot 1^3 + 1^2 + 2 \cdot 1 = 1+3+1+2 = 7 \equiv 2 \pmod{5}$ , so 1 is not a zero.

For  $x=2$ :  $2^5 + 3 \cdot 2^3 + 2^2 + 2 \cdot 2 = 32+24+4+4 = 64 \equiv 4 \pmod{5}$ , so 2 is not a zero.

For  $x=3$ :  $3^5 + 3 \cdot 3^3 + 3^2 + 2 \cdot 3 = 243+81+9+6 = 339 \equiv 4 \pmod{5}$ , so 3 is not a zero.

For  $x=4$ :  $4^5 + 3 \cdot 4^3 + 4^2 + 2 \cdot 4 = 1024+192+16+8 = 1240 \equiv 0 \pmod{5}$ , so 4 is a zero.

So the zeros of the polynomial in  $\mathbb{Z}_5$  are 0 and 4. The final answer is D.

\*\*\*\*\*

Answer Option 9:

In  $\mathbb{Z}_5$ , each element  $\{0, 1, 2, 3, 4\}$  is a root of the polynomial if when substituted into the polynomial results in zero.

For  $x=0$ :  $0^5+3 \cdot 0^3+0^2+2 \cdot 0 = 0$  which equals zero so,  $x=0$  is a root of the polynomial.

For  $x=1$ :  $1^5+3 \cdot 1^3+1^2+2 \cdot 1 = 1+3+1+2 = 7$  in  $\mathbb{Z}_5$  equals 2, so  $x=1$  is not a root of the polynomial.

For  $x=2$ :  $2^5+3 \cdot 2^3+2^2+2 \cdot 2 = 32+24+4+4 = 64$  in  $\mathbb{Z}_5$  equals 4, so  $x=2$  is not a root of the polynomial.

For  $x=3$ :  $3^5+3 \cdot 3^3+3^2+2 \cdot 3 = 243+81+9+6 = 339$  in  $\mathbb{Z}_5$  equals 4, so  $x=3$  is not a root of the polynomial.

For  $x=4$ :  $4^5+3 \cdot 4^3+4^2+2 \cdot 4 = 1024+192+16+8 = 1240$  in  $\mathbb{Z}_5$  equals 0, so  $x=4$  is a root of the polynomial.

So the zeros of the polynomial in the field  $\mathbb{Z}_5$  are 0 and 4. Final answer: D

\*\*\*\*\*

Question 4:

'Statement 1 | A factor group of a non-Abelian group is non-Abelian. Statement 2 | If K is a normal subgroup of H and H is a normal subgroup of G, then K is a normal subgroup of G.', A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1: False. The factor group of a non-Abelian group can be either Abelian or non-Abelian. For instance, consider the symmetric group  $S_3$  (which is non-Abelian) and its normal subgroup  $A_3$  (which is Abelian). The factor group  $S_3/A_3$  is isomorphic to  $\mathbb{Z}_2$ , an Abelian group.

Statement 2: True. This is a standard result in group theory. In general, if H is a normal subgroup of G and K is a normal subgroup of H, then K is a normal subgroup of G.

So, the correct answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 2:

Statement 1: False. A factor group of a non-Abelian group can be Abelian. For example, consider the group  $S_3$  (symmetric group of degree 3). The factor group  $S_3/A_3$  (where  $A_3$  is the alternating group of degree 3, a normal subgroup of  $S_3$ ) is a group of order 2, hence is Abelian.

Statement 2: True. The normality of subgroups is transitive. If K is a normal subgroup of H, and H is a normal subgroup of G, then K is a normal subgroup of G.

So, the correct answer is D. 'False, True'

\*\*\*\*\*

Answer Option 3:

Statement 1 is false. A factor group (also known as a quotient group) of a non-Abelian group can be Abelian. For example, consider the symmetric group  $S_3$  (which is non-Abelian) and its normal subgroup  $A_3$  (which is Abelian). The factor group  $S_3/A_3$  is isomorphic to  $\mathbb{Z}_2$ , which is Abelian.

Statement 2 is true. If K is a normal subgroup of H and H is a normal subgroup of G, then K is also a normal subgroup of G. This is because the definition of a normal subgroup (that it is invariant under conjugation by elements from the larger group) is transitive in this way.

So the correct answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 4:

Statement 1 | A factor group of a non-Abelian group is non-Abelian: This statement is false. A factor group of a non-Abelian group can be Abelian. For instance, consider the symmetric group  $S_3$  (which is non-Abelian). The factor group  $S_3/A_3$  (where  $A_3$  is the subgroup of even permutations) is isomorphic to  $\mathbb{Z}_2$ , which is Abelian.

Statement 2 | If K is a normal subgroup of H and H is a normal subgroup of G, then K is a normal subgroup of G: This statement is true. If K is a normal subgroup of H and H is a normal subgroup of G, then K is indeed a normal subgroup of G.

Final Answer: D

\*\*\*\*\*

Answer Option 5:

Statement 1: False. A factor group of a non-Abelian group can be Abelian. Consider the non-Abelian group  $S_3$ , the symmetric group of order 3, and its normal subgroup  $A_3$ , the alternating group of order 3. The factor group  $S_3/A_3$  is isomorphic to  $\mathbb{Z}_2$ , which is Abelian.

Statement 2: True. The normality of a subgroup is transitive. If K is normal in H and H is normal in G, then K is normal in G.

Final Answer: D. 'False, True'

\*\*\*\*\*

Answer Option 6:

Statement 1: A factor group of a non-Abelian group can be Abelian. Consider the group of integers under addition. It's an Abelian group and also a factor group of the non-Abelian symmetric group  $S_3$ . Hence, the first statement is False.

Statement 2: This is a known property of normal subgroups: If K is a normal subgroup of H and H is a normal subgroup of G, then K is a normal subgroup of G. Hence, the second statement is True.

So the answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 7:

Statement 1 is false. A factor group (or quotient group) of a non-Abelian group can be Abelian. For example, the factor group of the symmetric group  $S_3$  by its alternating subgroup  $A_3$  (which is also  $S_3$ ) is isomorphic to the group of integers modulo 2, which is an Abelian group.

Statement 2 is true. If K is a normal subgroup of H and H is a normal subgroup of G, then K is a normal subgroup of G. This is a standard result in group theory.

So, the final answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 8:

Statement 1: False. A factor group of a non-Abelian group can be Abelian. For instance, consider the non-Abelian group of symmetries of an equilateral triangle. The factor group by the subgroup of rotations is isomorphic to the cyclic group of order 2, which is Abelian.

Statement 2: True. If K is a normal subgroup of H and H is a normal subgroup of G, then K is indeed a normal subgroup of G. This follows from the definition of normal subgroups and can be shown using group actions.

So, the correct answer is D. 'False, True'. Final Answer: D

\*\*\*\*\*

Answer Option 9:

Statement 1 | The factor group (also known as the quotient group) of a non-Abelian group can be Abelian. A simple example is the group of integers under addition, which is Abelian, and is also the factor group of the group of integers under addition by the subgroup of even integers. So, Statement 1 is false.

Statement 2 | This statement is true. If  $K$  is a normal subgroup of  $H$  and  $H$  is a normal subgroup of  $G$ , then  $K$  is a normal subgroup of  $G$ . This follows from the definition of a normal subgroup, which is invariant under conjugation by elements of the group it is a subgroup of. In this case, any element  $g$  of  $G$  will conjugate  $K$  into itself, since it will conjugate  $H$  into itself and  $H$  in turn conjugates  $K$  into itself. So, Statement 2 is true.

So, the answer is D. 'False, True'.

\*\*\*\*\*

Question 5:

'Find the product of the given polynomials in the given polynomial ring.  $f(x) = 4x - 5$ ,  $g(x) = 2x^2 - 4x + 2$  in  $\mathbb{Z}_8[x]$ .'. A.  $2x^2 + 5$ , B.  $6x^2 + 4x + 6$ , C. '0', D.  $x^2 + 1$ '

=====

Answer Option 1:

The product of  $f(x)$  and  $g(x)$  in  $\mathbb{Z}_8[x]$  is  $8x^3 - 30x^2 + 20x - 10$ . Simplifying, we obtain  $8x^3 - 40x^2 + 40x - 10$ .

In  $\mathbb{Z}_8[x]$ , we can reduce all coefficients modulo 8, so the result is  $0x^3 + 0x^2 + 0x - 2 = \boxed{0}$ . Final Answer: C

=====

Answer Option 2:

In  $\mathbb{Z}_8[x]$ , we perform arithmetic modulo 8. So,  $f(x)g(x) = (4x - 5)(2x^2 - 4x + 2) = 8x^3 - 20x^2 + 8x - 10$ . This simplifies to  $0x^3 + 0x^2 + 0x - 2$  in  $\mathbb{Z}_8[x]$ , which further simplifies to 6. So, the product of the given polynomials in the given polynomial ring is the constant polynomial '6'. Since '6' is not an option, our product is closest to option C: '0'. Final answer: C.

=====

Answer Option 3:

The polynomial ring  $\mathbb{Z}_8[x]$  uses arithmetic modulo 8, so all coefficients should be reduced mod 8. The product of  $f(x)$  and  $g(x)$  is  $(4x - 5)(2x^2 - 4x + 2) = 8x^3 - 16x^2 + 8x - 10x^2 + 20x - 10 = 8x^3 - 26x^2 + 28x - 10$ . Reducing mod 8, we get  $0x^3 + 6x^2 + 4x + 6 = 6x^2 + 4x + 6$ . Hence, the final answer is B.  $6x^2 + 4x + 6$ .

=====

Answer Option 4:

In the ring  $\mathbb{Z}_8[x]$ , we have 8 as the modulus. Therefore, the product of the given polynomials  $f(x)$  and  $g(x)$  is  $(4x - 5)(2x^2 - 4x + 2) = 8x^3 - 20x^2 + 8x + 10$ . In the ring  $\mathbb{Z}_8[x]$ , any multiple of 8 is equivalent to 0, so  $8x^3 - 20x^2 + 8x + 10$  is equivalent to  $0x^3 + 4x^2 + 0x + 2$ , which simplifies to  $4x^2 + 2$ . Therefore, the final answer is B.  $6x^2 + 4x + 6$ .

=====

Answer Option 5:

The product of the polynomials is  $f(x)g(x) = (4x - 5)(2x^2 - 4x + 2) = 8x^3 - 20x^2 + 8x - 10x^2 + 20x - 10 = 8x^3 - 30x^2 + 28x - 10$ . Now, to find the equivalent polynomial in  $\mathbb{Z}_8[x]$ , we must reduce each coefficient modulo 8. This gives us  $0x^3 + 6x^2 + 4x + 6 = 6x^2 + 4x + 6$ .

Final answer: B

=====

Answer Option 6:

To perform the multiplication, we simply distribute each term in  $f(x)$  to every term in  $g(x)$ , and then collect like terms:

$$\begin{aligned} f(x)g(x) &= (4x - 5)(2x^2 - 4x + 2) \\ &= 8x^3 - 16x^2 + 8x - 10x^2 + 20x - 10 \\ &= 8x^3 - 26x^2 + 28x - 10. \end{aligned}$$

We then reduce each coefficient modulo 8:

$$\begin{aligned} &= 8x^3 + 2x^2 + 4x + 6 \\ &= 0 + 2x^2 + 4x + 6 \\ &= 2x^2 + 4x + 6. \end{aligned}$$

Therefore the product of these polynomials in  $\mathbb{Z}_8[x]$  is  $2x^2 + 4x + 6$ . Final Answer: B

=====

Answer Option 7:

The product of the polynomials in the ring  $\mathbb{Z}_8[x]$  is the same as the product in  $\mathbb{Z}[x]$  with the coefficients reduced modulo 8. We can compute this product as follows:

$$\begin{aligned} f(x)g(x) &= (4x - 5)(2x^2 - 4x + 2) \\ &= 8x^3 - 16x^2 + 8x - 10x^2 + 20x - 10 \\ &= 8x^3 - 26x^2 + 28x - 10 \end{aligned}$$

Reduce modulo 8:

$$= 0 - 2x^2 + 4x + 6$$

So the product is  $-2x^2 + 4x + 6$  in  $\mathbb{Z}_8[x]$  which corresponds to  $6x^2 + 4x + 6$ .

Hence, the answer is B.  $6x^2 + 4x + 6$ .

=====

Answer Option 8:

The product of the two polynomials is  $f(x)g(x) = (4x - 5)(2x^2 - 4x + 2) = 8x^3 - 16x^2 + 8x - 10x^2 + 20x - 10$ .

In  $\mathbb{Z}_8[x]$ , we have to reduce everything modulo 8. This gives us:

$$8x^3 - 16x^2 + 8x - 10x^2 + 20x - 10 = 0x^3 - 2x^2 + 4x + 6 = -2x^2 + 4x + 6.$$

Now, we need to get rid of the negative sign on the  $-2x^2$  term, which we can do by adding 8, because 8 is equivalent to 0 in  $\mathbb{Z}_8[x]$ . This gives us  $6x^2 + 4x + 6$ .

So, the product of the two polynomials, when considered in the polynomial ring  $\mathbb{Z}_8[x]$ , is  $\boxed{6x^2 + 4x + 6}$ .

Final Answer: B

=====



Answer Option 9:

Multiplication in a polynomial ring is just like normal polynomial multiplication, except that all coefficients are reduced modulo the order of the ring after each step.

So we compute the product  $f(x)g(x) = (4x - 5)(2x^2 - 4x + 2)$ .

This gives:

$$= 8x^3 - 16x^2 + 8x - 10x^2 + 20x - 10$$

$$= 8x^3 - 26x^2 + 28x - 10$$

Reducing each coefficient modulo 8 we get:

$$= 0x^3 + 6x^2 + 4x + 6$$

So the product  $f(x)g(x)$  in  $\mathbb{Z}_8[x]$  is  $6x^2 + 4x + 6$

Final answer: B

\*\*\*\*\*

Question 6:

'Statement 1 | If a group has an element of order 15 it must have at least 8 elements of order 15. Statement 2 | If a group has more than 8 elements of order 15, it must have at least 16 elements of order 15.'

A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1 is true. If a group has an element of order 15, say  $a$ , then  $a, a^2, \dots, a^{14}$  are distinct elements of the group and have order 15.

Statement 2 is false. The group can have more than 8 elements of order 15, but it is still possible for it to have fewer than 16 elements of order 15.

Final Answer: C. 'True, False'

=====

Answer Option 2:

Statement 1 is True. If a group has an element of order 15, it must have at least 8 elements of order 15. This is because if  $g$  is an element of order  $n$  in a group, then  $g, g^2, g^3, \dots, g^{n-1}$  are all different elements of the group of order  $n$ .

Statement 2 is False. The number of elements of a certain order in a group does not necessarily have to be a multiple of any specific number. Hence, it is not necessary that if a group has more than 8 elements of order 15, it must have at least 16 elements of order 15.

Final Answer: C

=====

Answer Option 3:

Statement 1 is true. When a group has an element  $a$  of order 15, there will be 15 distinct powers of  $a$  (including the identity) in the group. The order of all non-identity powers of  $a$  must also be 15. Thus, the group must have at least 14 elements of order 15.

Statement 2 is false. It's possible for a group to have exactly 9 elements of order 15. Consider a cyclic group of order 15, for example. It has exactly 8 elements of order 15 (the non-identity powers of a generator), and including the identity gives 9 elements of order 15 without needing to go up to 16.

Therefore, the correct answer is C. 'True, False'.

=====

Answer Option 4:

Statement 1: True. If a group has an element of order 15, it must have its inverse (which is also of order 15) and the elements generated by it (which is of order 15), therefore the group must have at least 8 elements of order 15.

Statement 2: False. Assuming there are more than 8 elements of order 15 in the group, it doesn't necessarily mean that there must be at least 16. One can construct a group with 9 elements of order 15.

Final Answer: C

=====

Answer Option 5:

Statement 1 is True. The order of an element in group theory is the smallest positive integer  $n$  such that  $a^n = e$ , where  $e$  is the identity element of the group and  $a$  is any element of the group. If a group has an element of order 15, it must also have its inverses and powers, which are distinct, hence it would have at least 8 elements of order 15 (the element, its inverse, and their powers up to the 7th).

Statement 2 is False. Having more than 8 elements of order 15 does not necessarily imply that it must have at least 16 elements of order 15. In group theory, the existence of elements of a certain order does not necessarily guarantee the existence of a certain number of elements of that order. Therefore, the answer is C. 'True, False'.

=====

Answer Option 6:

Statement 1: True. If a group has an element of order 15, it must have an element of each power up to 14 (and the identity), which are also of order 15. This gives 15 elements of order 15, so the group must have at least 8.

Statement 2: True. If a group has more than 15 elements of order 15, then the elements must come in pairs (each element and its inverse). If there are more than 8 pairs, there must be at least 16 elements of order 15.

Final Answer: A

=====

Answer Option 7:

Statement 1 is true. In a group, if there is an element of order 15, call it  $a$ , then there must be 15 elements generated by  $a$  (all the powers of  $a$  from 1 to 14 and the identity), and among these,  $15-1 = 14$  elements will be of order 15. So the group has at least 8 elements of order 15.

Statement 2 is also true. If a group has more than 8 elements of order 15, then it must have more than one element of order 15 (since one element of order 15 can generate at most 14 elements of order 15 as described above). If there are two elements of order 15, then there would be a total of  $2 \cdot 14 = 28$  elements of order 15. So, if a group has more than 8 elements of order 15, it must have at least 16 elements of order 15.

So the correct final answer is A. 'True, True'

=====

Answer Option 8:

Statement 1: True. In a group, the order of an element divides the order of the group. If a group has an element of order 15, its order must be a multiple of 15. In a group of order 15, there are exactly two elements of order 15 (the identity element and the element of order 15 itself). However, the identity element has order 1, not 15. So, there must be at least 8 elements of order 15 (the element itself and its 14 powers).

non-identity powers).

Statement 2: False. A group could have exactly 9 elements of order 15 (the element itself and its 8 non-identity powers), so it is not necessary to have at least 16 elements of order 15 if there are more than 8.

So, the final answer is C. 'True, False'

\*\*\*\*\*

Answer Option 9:

Statement 1 is true. In group theory, if a group has an element of order 15, it must have at least 8 such elements. This is because the order of a group is the smallest positive integer such that raising the group element to that power gives the identity. So if a group has an element of order 15, it must contain all the powers of that element up to the 14th power. Half of these elements - the powers of 1, 3, 5, 7, 9, 11, 13 - are of order 15.

Statement 2 is also true. The reasoning is similar to that of Statement 1. If a group has more than 8 elements of order 15, it must have at least 16 such elements. This is because elements of order 15 come in pairs. If one element's order is 15, then its inverse's order is also 15, which means that for every element of order 15, there is another element of order 15.

Final Answer: A

\*\*\*\*\*

Question 7:

'Statement 1 | Every homomorphic image of a group  $G$  is isomorphic to a factor group of  $G$ . Statement 2 | The homomorphic images of a group  $G$  are the same (up to isomorphism) as the factor groups of  $G$ .'

A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1 is true. By the first isomorphism theorem, the image of any group homomorphism is isomorphic to the factor group of the domain by the kernel of the homomorphism.

Statement 2 is false. Not every factor group of a given group  $G$  can be realized as the image of a group homomorphism defined on  $G$ . In other words, there are factor groups of  $G$  that are not homomorphic images of  $G$ .

Final answer: C. 'True, False'

\*\*\*\*\*

Answer Option 2:

Statement 1 is true. Given a homomorphism from a group  $G$  to a group  $G'$ , the kernel of this homomorphism is a normal subgroup of  $G$ . The factor group formed by this kernel is isomorphic to  $G'$ .

Statement 2 is false. Not every factor group of  $G$  is isomorphic to a homomorphic image of  $G$ . There may be factor groups of  $G$  that do not correspond to the image of a homomorphism.

So, the final answer is C. 'True, False'.

\*\*\*\*\*

Answer Option 3:

Statement 1 is true. Every homomorphic image of a group  $G$  is indeed isomorphic to a factor group of  $G$ . This is a standard result from group theory.

Statement 2 is false. While every homomorphic image of a group  $G$  is isomorphic to some factor group of  $G$ , not every factor group of  $G$  is a homomorphic image of  $G$ . The homomorphic images of  $G$  are a subset of the factor groups of  $G$ , but they may not be the entirety of the factor groups.

Therefore, the answer is C. 'True, False'

\*\*\*\*\*

Answer Option 4:

Statement 1 is true: every homomorphic image of a group  $G$  is isomorphic to a factor group of  $G$ . This is a consequence of the First Isomorphism Theorem.

Statement 2 is false: the homomorphic images of a group  $G$  are not necessarily the same as the factor groups of  $G$ . A factor group is defined for a particular normal subgroup of  $G$ , but a homomorphic image could be any group that is the image of a homomorphism from  $G$ , not just those that correspond to factor groups.

So the final answer is C. 'True, False'.

\*\*\*\*\*

Answer Option 5:

Statement 1 is true. If there is a homomorphism from  $G$  to  $H$ , then the image of  $G$ , which is a subgroup of  $H$ , is isomorphic to the factor group  $G/K$ , where  $K$  is the kernel of the homomorphism.

Statement 2 is false. Not every factor group of  $G$  has to be a homomorphic image of  $G$ . For example, take  $G$  to be the group of integers, and let the factor group be the integers modulo 2. There is no homomorphism from the integers to this factor group that is onto.

So, the correct option is C. 'True, False'

\*\*\*\*\*

Answer Option 6:

Statement 1 is true. This is the fundamental property of the first isomorphism theorem for groups: If  $\phi: G \rightarrow H$  is a group homomorphism, then the image of  $\phi$  in  $H$  is isomorphic to the factor group  $G/\ker(\phi)$ .

Statement 2 is false. While every homomorphic image of a group  $G$  is isomorphic to some factor group of  $G$  (as seen in statement 1), not every factor group of  $G$  is a homomorphic image of  $G$ . There may be factor groups of  $G$  that do not correspond to any homomorphism from  $G$ .

So the correct answer is C. 'True, False'.

\*\*\*\*\*

Answer Option 7:

Statement 1 is true because every homomorphism from a group  $G$  to another group  $H$ , induces a normal subgroup  $K$  of  $G$  such that  $G/K$  is isomorphic to the image of the homomorphism (the First Isomorphism Theorem).

Statement 2 is false because not all factor groups are homomorphic images of  $G$ . A factor group is formed by considering the cosets of a normal subgroup of a group  $G$ , but the homomorphic image of  $G$  is defined by a homomorphism from  $G$  to another group, and not every factor group can be realized this way.

Therefore, the correct answer is (C) 'True, False'. Final Answer: C

\*\*\*\*\*

Answer Option 8:

The first statement says that every homomorphic image of a group  $G$  is isomorphic to a factor group of  $G$ . This is true. Given any homomorphism  $\phi: G \rightarrow H$ , the image of  $\phi$  is isomorphic to the factor group  $G/\ker(\phi)$ , where  $\ker(\phi)$  is the kernel of  $\phi$ .

The second statement says that the homomorphic images of a group  $G$  are the same (up to isomorphism) as the factor groups of  $G$ . This is false. There are factor groups of  $G$  that are not homomorphic images of  $G$ .

So the correct answer is C: 'True, False'.

\*\*\*\*\*

Answer Option 9:

Statement 1 is true: every homomorphic image of a group  $G$  is isomorphic to a factor group of  $G$ . This follows from the First Isomorphism Theorem, which states that if  $\phi: G \rightarrow H$  is a group homomorphism, then the image of  $\phi$  is isomorphic to the factor group  $G/\ker(\phi)$ , where  $\ker(\phi)$  is the kernel of  $\phi$ .

Statement 2 is false: the homomorphic images of a group  $G$  are not necessarily the same as the factor groups of  $G$ . While it is true that every homomorphic image of  $G$  is isomorphic to some factor group of  $G$ , not every factor group of  $G$  is necessarily a homomorphic image of  $G$ .

So the final answer is C. 'True, False'.

\*\*\*\*\*

Question 8:

'Statement 1 | A ring homomorphism is one to one if and only if the kernel is  $\{0\}$ . Statement 2 |  $Q$  is an ideal in  $R$ .'. A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1 is True. This is a standard result in ring theory: a ring homomorphism is injective if and only if its kernel is the zero ideal.

Statement 2 is False as it stands. Whether  $Q$  is an ideal in  $R$  or not depends on the specific structures of  $Q$  and  $R$ . Without further information, we cannot say for certain that  $Q$  is an ideal in  $R$ .

So, the final answer is C: 'True, False'.

=====

Answer Option 2:

Statement 1 is true. In ring theory, the kernel of a ring homomorphism is the set of elements that map to the additive identity in the codomain. A ring homomorphism is injective (one to one) if and only if its kernel is  $\{0\}$ .

Statement 2 is false.  $Q$  and  $R$  are fields, and the only ideals in a field are the zero ideal and the field itself.  $Q$  cannot be an ideal in  $R$  unless  $Q = R$  or  $Q$  is the zero ideal, neither of which are generally true.

So, the answer is C. 'True, False'.

=====

Answer Option 3:

Statement 1 is true. In ring theory, a homomorphism is one to one if and only if the kernel (the set of elements that are mapped to the additive identity in the target ring) is  $\{0\}$ .

Statement 2 is incomplete and hence it cannot be determined as true or false. It doesn't specify what  $Q$  and  $R$  are. If  $Q$  and  $R$  are rings and  $Q$  is a subset of  $R$ , then  $Q$  could be an ideal in  $R$  if it satisfies the ideal properties. But without specific information, it's impossible to concretely say if the statement is true or false.

So the final answer is C. 'True, False'.

=====

Answer Option 4:

Statement 1 is True. In ring theory, a ring homomorphism is a function between two rings which respects the structure. The kernel of a ring homomorphism is the inverse image of 0, and if the kernel is  $\{0\}$ , it means that only 0 gets mapped to 0, hence the function is one to one.

Statement 2 is False. The set of rational numbers  $Q$  is a field, and as such, it can't be an ideal in any ring  $R$  unless  $R = Q$  itself because the only ideals in a field are the field itself and the zero ideal.

So, the correct answer is C. 'True, False'

=====

Answer Option 5:

Statement 1: True. In ring theory, a ring homomorphism is a function between two rings which respects the structure. The kernel of a ring homomorphism is the set of elements that map to zero. A ring homomorphism is injective if and only if its kernel is the trivial ideal  $\{0\}$ .

Statement 2: False. This statement is vague because it doesn't specify what  $Q$  and  $R$  are. Assuming  $Q$  and  $R$  are rings, it's not necessarily true that  $Q$  is an ideal in  $R$ . An ideal is a subset of a ring which is closed under addition and multiplication by the ring. Not all rings are ideals of other rings.

Final answer: C

=====

Answer Option 6:

Statement 1 is true. In ring theory, it is a standard fact that a ring homomorphism is one to one if and only if its kernel (the set of elements that map to zero) is  $\{0\}$ .

Statement 2 is false without more context.  $Q$  and  $R$  are usually used to denote the sets of rational and real numbers, respectively, but whether  $Q$  is an ideal in  $R$  depends on the operations defined on  $R$ . The standard operations on the real numbers do not make  $Q$  an ideal in  $R$  because, for instance, the product of a rational number and an irrational number (which is an element of  $R$  but not of  $Q$ ) is not necessarily in  $Q$ .

Hence, the final answer is C. 'True, False'

=====

Answer Option 7:

Statement 1: A ring homomorphism is one to one if and only if the kernel is  $\{0\}$ . This statement is True. In ring theory, the kernel of a ring homomorphism is the set of elements that map to zero in the image. A homomorphism is injective (one-to-one) if and only if its kernel is  $\{0\}$ .

Statement 2:  $Q$  is an ideal in  $R$ . This statement is False. The set of rational numbers ( $Q$ ) is not an ideal in the ring of real numbers ( $R$ ). An ideal in a ring  $R$  is a subset that is closed under addition and under multiplication by elements in  $R$ . But  $Q$  is not closed under multiplication by elements in  $R$ , because the product of a rational number and an irrational number is irrational.

So the final answer is C. 'True, False'

=====

Answer Option 8:

Statement 1 is true. In ring theory, the kernel of a ring homomorphism is the set of all elements that map to the additive identity in the codomain. If only the zero element of the domain maps to the zero element of the codomain (i.e., if the kernel is  $\{0\}$ ), then the homomorphism is one to one.

Statement 2 is false. The statement doesn't provide enough information.  $Q$  and  $R$  are not specified - they could be any rings. In general, an ideal is a subset of a ring that is closed under subtraction and multiplication by elements in the ring. Without additional information, we can't say whether  $Q$  is an ideal in  $R$ .

So, the correct answer is C. 'True, False'.

\*\*\*\*\*

Answer Option 9:

Statement 1 is true. In ring theory, a ring homomorphism is a function between two rings which respects the operations of addition and multiplication. The kernel of a ring homomorphism is the set of elements that map to the additive identity in the codomain. A ring homomorphism is one-to-one if and only if its kernel is the set containing only the additive identity.

Statement 2 is vague without context, because it doesn't specify what  $R$  and  $Q$  are. However, in most contexts (like when  $R$  is a ring and  $Q$  is a set), this statement would be false. An ideal in a ring  $R$  is a subset  $Q$  of  $R$  that is closed under the operations of  $R$  and absorbs products from  $R$ , but we don't have enough information to determine if  $Q$  is an ideal in  $R$  in this situation.

So, the answer is C. 'True, False'.

\*\*\*\*\*

Question 9:

'Find the degree for the given field extension  $\mathbb{Q}(\sqrt{2} + \sqrt{3})$  over  $\mathbb{Q}$ .' A. '0', B. '4', C. '2', D. '6'

=====

Answer Option 1:

The extension  $\mathbb{Q}(\sqrt{2} + \sqrt{3})$  over  $\mathbb{Q}$  has degree 4.

This can be proven by showing that the minimal polynomial for  $\sqrt{2} + \sqrt{3}$  over  $\mathbb{Q}$  is  $x^4 - 10x^2 + 1$ , which has degree 4. Hence, the extension field generated by  $\sqrt{2} + \sqrt{3}$  over  $\mathbb{Q}$  will have degree 4.

Final answer: B.

=====

Answer Option 2:

The degree of the extension  $\mathbb{Q}(\sqrt{2} + \sqrt{3})$  over  $\mathbb{Q}$  is 4. This can be shown by considering the minimal polynomial of  $\sqrt{2} + \sqrt{3}$  over  $\mathbb{Q}$ , which is  $x^4 - 10x^2 + 1$ . This polynomial is irreducible over  $\mathbb{Q}$ , hence its degree gives the degree of the field extension. Final Answer: B.

=====

Answer Option 3:

The degree of the field extension  $\mathbb{Q}(\sqrt{2} + \sqrt{3})$  over  $\mathbb{Q}$  is 4. This is because  $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$ , so the minimal polynomial of  $\sqrt{2} + \sqrt{3}$  over  $\mathbb{Q}$  is  $x^4 - 10x^2 + 1$ , which is irreducible over  $\mathbb{Q}$  and thus the degree of the field extension is the degree of the minimal polynomial, which is 4. Final Answer: B.

=====

Answer Option 4:

The minimal polynomial for  $\sqrt{2} + \sqrt{3}$  over  $\mathbb{Q}$  is  $x^4 - 10x^2 + 1 = 0$ . One can verify this by noting that  $\sqrt{2} + \sqrt{3}$  is a root and that the polynomial is irreducible over  $\mathbb{Q}$ . So the degree of the extension  $\mathbb{Q}(\sqrt{2} + \sqrt{3})$  over  $\mathbb{Q}$  is 4. Final Answer: B

=====

Answer Option 5:

The degree of a field extension is the degree of the minimal polynomial of the field over its base field.

It is not hard to check that the polynomial  $p(x) = x^4 - 10x^2 + 1$  has  $\sqrt{2} + \sqrt{3}$  as a root, and in fact this is the minimal polynomial of  $\sqrt{2} + \sqrt{3}$  over  $\mathbb{Q}$ .

Hence, the degree for the given field extension  $\mathbb{Q}(\sqrt{2} + \sqrt{3})$  over  $\mathbb{Q}$  is  $\boxed{4}$ . Final Answer: B

=====

Answer Option 6:

The degree of the extension is the degree of the minimal polynomial of  $\sqrt{2} + \sqrt{3}$  over  $\mathbb{Q}$ . Consider the polynomial  $(x^2 - 2\sqrt{2}x - 1)(x^2 + 2\sqrt{2}x - 1) = x^4 - 10x^2 + 1$ . This is the same as  $(x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3})$  (note that all the roots of this polynomial are  $\pm\sqrt{2} \pm \sqrt{3}$ ). Therefore, the degree of the field extension is  $\boxed{4}$ , and the answer is B.

=====

Answer Option 7:

The degree of the field extension  $\mathbb{Q}(\sqrt{2} + \sqrt{3})$  over  $\mathbb{Q}$  is equal to the degree of the minimal polynomial of  $\sqrt{2} + \sqrt{3}$  over  $\mathbb{Q}$ . We can find this polynomial by noticing that  $(\sqrt{2} + \sqrt{3})^2 = 2 + 2\sqrt{6} + 3$  and  $(\sqrt{2} + \sqrt{3})^4 = 49 + 20\sqrt{6}$ . Thus,  $\sqrt{2} + \sqrt{3}$  is a root of the polynomial  $x^4 - 10x^2 + 1 = 0$ , and it's easy to check that this polynomial is irreducible over  $\mathbb{Q}$ . Thus, the degree of the field extension is  $\boxed{4}$ . Final Answer: B

=====

Answer Option 8:

The degree of the extension is 4.

We know that  $\mathbb{Q}(\sqrt{2} + \sqrt{3})$  is a subset of  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  and that  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ , so  $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] \leq 4$ .

We also know that  $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$  and  $(\sqrt{2} + \sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3}$ , so  $\sqrt{2}$  and  $\sqrt{3}$  are in  $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ . This means that  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$ .

Therefore,  $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$  and  $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ .

Final Answer: B

=====

Answer Option 9:

The degree of a field extension is the dimension of the larger field as a vector space over the smaller field. In this case, we want to find the degree of  $\mathbb{Q}(\sqrt{2} + \sqrt{3})$  over  $\mathbb{Q}$ .

First, we note that  $\mathbb{Q}(\sqrt{2} + \sqrt{3})$  must contain  $\sqrt{2}$  and  $\sqrt{3}$ . However,  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3})$  because  $\sqrt{2} = \frac{\sqrt{2} + \sqrt{3} + \sqrt{2} - \sqrt{3}}{2}$  and  $\sqrt{3} = \frac{\sqrt{2} + \sqrt{3} - (\sqrt{2} - \sqrt{3})}{2}$ .

We know that  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  has degree 4 over  $\mathbb{Q}$  because  $\sqrt{2}$  and  $\sqrt{3}$  are both roots of 2nd degree polynomials with rational coefficients ( $x^2 - 2$  and  $x^2 - 3$ , respectively) that are irreducible over  $\mathbb{Q}$ , and the minimal polynomial for  $\sqrt{2}$  and  $\sqrt{3}$  over  $\mathbb{Q}$  has degree 4 ( $x^4 - 10x^2 + 1$ ).

Therefore, the degree of  $\mathbb{Q}(\sqrt{2} + \sqrt{3})$  over  $\mathbb{Q}$  is 4. The final answer is B.

=====



Question 10:

'Find all zeros in the indicated finite field of the given polynomial with coefficients in that field.  $x^3 + 2x + 2$  in  $\mathbb{Z}_7$ , A. '1', B. '2', C. '2,3', D. '6'

=====

Answer Option 1:

Substituting all elements of  $\mathbb{Z}_7$  into the polynomial, we find that the polynomial is zero if and only if  $x = 1$  or  $x = 6$ . Thus the solution is  $\boxed{1, 6}$ . Final Answer: D

\*\*\*\*\*

Answer Option 2:

Substituting all the elements of  $\mathbb{Z}_7$  in the polynomial, we have:

$$P(0) = 2$$

$$P(1) = 1^3 + 2^1 + 2 = 5$$

$$P(2) = 2^3 + 2^2 + 2 = 14 \equiv 0 \pmod{7}$$

$$P(3) = 3^3 + 2^3 + 2 = 35 \equiv 0 \pmod{7}$$

$$P(4) = 4^3 + 2^4 + 2 = 72 \not\equiv 0 \pmod{7}$$

$$P(5) = 5^3 + 2^5 + 2 = 137 \not\equiv 0 \pmod{7}$$

$$P(6) = 6^3 + 2^6 + 2 = 230 \not\equiv 0 \pmod{7}$$

So, the zeros of the polynomial are 2 and 3. Final Answer: C

\*\*\*\*\*

Answer Option 3:

The zeros of the polynomial over the field  $\mathbb{Z}_7$  are the  $x$ -values that satisfy the given polynomial equation. We can compute  $x^3 + 2x + 2$  for each value from 0 to 6, because those are all the elements in  $\mathbb{Z}_7$ .

$$x=0: 0^3 + 2^0 + 2 = 2$$

$$x=1: 1^3 + 2^1 + 2 = 5$$

$$x=2: 2^3 + 2^2 + 2 = 6$$

$$x=3: 3^3 + 2^3 + 2 = 6$$

$$x=4: 4^3 + 2^4 + 2 = 4$$

$$x=5: 5^3 + 2^5 + 2 = 4$$

$$x=6: 6^3 + 2^6 + 2 = 0$$

So the only value of  $x$  that makes the polynomial  $x^3 + 2x + 2$  equal to zero in  $\mathbb{Z}_7$  is  $x=6$ . Final Answer: D

\*\*\*\*\*

Answer Option 4:

We can simply test each of the seven elements of  $\mathbb{Z}_7$ :

$\begin{aligned} & \backslash \text{begin{align*}} \end{aligned}$

$$0^3 + 2 \cdot 0 + 2 \equiv 2 \pmod{7}, \backslash \backslash$$

$$1^3 + 2 \cdot 1 + 2 \equiv 5 \pmod{7}, \backslash \backslash$$

$$2^3 + 2 \cdot 2 + 2 \equiv 6 \pmod{7}, \backslash \backslash$$

$$3^3 + 2 \cdot 3 + 2 \equiv 6 \pmod{7}, \backslash \backslash$$

$$4^3 + 2 \cdot 4 + 2 \equiv 0 \pmod{7}, \backslash \backslash$$

$$5^3 + 2 \cdot 5 + 2 \equiv 0 \pmod{7}, \backslash \backslash$$

$$6^3 + 2 \cdot 6 + 2 \equiv 0 \pmod{7}.$$

$\backslash \text{end{align*}}$ Therefore, the zeroes of this polynomial in  $\mathbb{Z}_7$  are  $\boxed{4, 5, 6}$ .

\*\*\*\*\*

Answer Option 5:

To find the zeros in the finite field, we substitute each element of  $\mathbb{Z}_7$  (i.e., each of the integers from 0 to 6) into the polynomial and see for which values the polynomial equals 0.

Substituting these values in, we get:

$$\text{For } x = 0: 0^3 + 2^0 + 2 = 2$$

$$\text{For } x = 1: 1^3 + 2^1 + 2 = 5$$

$$\text{For } x = 2: 2^3 + 2^2 + 2 = 12 \equiv 5 \pmod{7}$$

$$\text{For } x = 3: 3^3 + 2^3 + 2 = 35 \equiv 0 \pmod{7}$$

$$\text{For } x = 4: 4^3 + 2^4 + 2 = 74 \equiv 4 \pmod{7}$$

$$\text{For } x = 5: 5^3 + 2^5 + 2 = 135 \equiv 3 \pmod{7}$$

$$\text{For } x = 6: 6^3 + 2^6 + 2 = 224 \equiv 0 \pmod{7}$$

So, in the field  $\mathbb{Z}_7$ , the polynomial  $x^3 + 2x + 2$  has zeros at  $x = 3$  and  $x = 6$ . Therefore, the correct answer is D. '6'.

\*\*\*\*\*

Answer Option 6:

We can find the roots of the polynomial by plugging in the numbers from  $0$  to  $6$  (the elements of  $\mathbb{Z}_7$ ) and checking when the polynomial equals zero.

When  $x=0$ ,  $x^3+2x+2=2$ .

When  $x=1$ ,  $x^3+2x+2=1+2+2=5$ .

When  $x=2$ ,  $x^3+2x+2=2^3+2*2+2=8+4+2=14\equiv 0 \pmod{7}$ .

When  $x=3$ ,  $x^3+2x+2=3^3+2*3+2=27+6+2=35\equiv 0 \pmod{7}$ .

When  $x=4$ ,  $x^3+2x+2=4^3+2*4+2=64+8+2=74\equiv 5 \pmod{7}$ .

When  $x=5$ ,  $x^3+2x+2=5^3+2*5+2=125+10+2=137\equiv 6 \pmod{7}$ .

When  $x=6$ ,  $x^3+2x+2=6^3+2*6+2=216+12+2=230\equiv 2 \pmod{7}$ .

So, the roots are  $\boxed{2,3}$ . Final Answer: C

\*\*\*\*\*

Answer Option 7:

To find the zeroes of the polynomial, we substitute each element of  $\mathbb{Z}_7$  into the polynomial and see if it equals 0.

Substituting 0, 1, 2, 3, 4, 5, 6 we have:

For 0:  $0^3 + 2(0) + 2 = 2 \not\equiv 0$ , so 0 is not a root.

For 1:  $1^3 + 2(1) + 2 = 5 \not\equiv 0$ , so 1 is not a root.

For 2:  $2^3 + 2(2) + 2 = 14 \equiv 0 \pmod{7}$ , so 2 is a root.

For 3:  $3^3 + 2(3) + 2 = 35 \equiv 0 \pmod{7}$ , so 3 is a root.

For 4:  $4^3 + 2(4) + 2 = 74 \not\equiv 0 \pmod{7}$ , so 4 is not a root.

For 5:  $5^3 + 2(5) + 2 = 135 \not\equiv 0 \pmod{7}$ , so 5 is not a root.

For 6:  $6^3 + 2(6) + 2 = 224 \not\equiv 0 \pmod{7}$ , so 6 is not a root.

Hence, the roots of the polynomial in  $\mathbb{Z}_7$  are 2 and 3. Final Answer: C

\*\*\*\*\*

Answer Option 8:

To find the zeros of the given polynomial in  $\mathbb{Z}_7$ , we substitute each of the seven elements of  $\mathbb{Z}_7$  (0, 1, 2, 3, 4, 5, 6) into the polynomial and see which ones make it zero.

Substituting these values, we get:

For  $x = 0$ ,  $f(0) = 2$

For  $x = 1$ ,  $f(1) = 1^3 + 2*1 + 2 = 5$

For  $x = 2$ ,  $f(2) = 2^3 + 2*2 + 2 = 12 \equiv 5 \pmod{7}$

For  $x = 3$ ,  $f(3) = 3^3 + 2*3 + 2 = 35 \equiv 0 \pmod{7}$

For  $x = 4$ ,  $f(4) = 4^3 + 2*4 + 2 = 74 \equiv 4 \pmod{7}$

For  $x = 5$ ,  $f(5) = 5^3 + 2*5 + 2 = 137 \equiv 6 \pmod{7}$

For  $x = 6$ ,  $f(6) = 6^3 + 2*6 + 2 = 224 \equiv 0 \pmod{7}$

So, the zeros of the polynomial in  $\mathbb{Z}_7$  are 3 and 6. Final Answer: D

\*\*\*\*\*

Answer Option 9:

We can find all zeros of the polynomial by plugging in all possible elements of the field  $\mathbb{Z}_7$  which are 0, 1, 2, 3, 4, 5, 6.

If we plug in these values into the polynomial  $x^3 + 2x + 2$ , we get:

For 0:  $0^3 + 2*0 + 2 = 2$  which is not equal to 0.

For 1:  $1^3 + 2*1 + 2 = 5$  which is not equal to 0.

For 2:  $2^3 + 2*2 + 2 = 8 + 4 + 2 = 14 \equiv 0 \pmod{7}$

For 3:  $3^3 + 2*3 + 2 = 27 + 6 + 2 = 35 \equiv 0 \pmod{7}$

For 4:  $4^3 + 2*4 + 2 = 64 + 8 + 2 = 74$  which is not equal to 0 (mod 7).

For 5:  $5^3 + 2*5 + 2 = 125 + 10 + 2 = 137$  which is not equal to 0 (mod 7).

For 6:  $6^3 + 2*6 + 2 = 216 + 12 + 2 = 230$  which is not equal to 0 (mod 7).

Therefore, the zeros of the polynomial  $x^3 + 2x + 2$  in  $\mathbb{Z}_7$  are 2 and 3. Final Answer: C

\*\*\*\*\*

Question 11:

'Statement 1 | If  $H$  is a subgroup of  $G$  and  $a$  belongs to  $G$  then  $|aH| = |Ha|$ . Statement 2 | If  $H$  is a subgroup of  $G$  and  $a$  and  $b$  belong to  $G$ , then  $aH$  and  $bH$  are identical or disjoint.', A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1 is true. The left and right cosets of an element in the group have the same order.

Statement 2 is also true. This is a property of cosets in group theory. Two cosets are either identical or they have no elements in common.

Therefore, the correct answer is A. 'True, True'.

\*\*\*\*\*

Answer Option 2:

Statement 1 is true. In group theory, for any subgroup  $H$  of a group  $G$ , and for any element  $a$  in  $G$ , the right and left cosets of  $H$  in  $G$  (defined by  $aH$  and  $Ha$  respectively) have the same size (or cardinality).

Statement 2 is also true. This is known as the Coset Theorem, which states that for any subgroup  $H$  of a group  $G$ , and for any elements  $a$  and  $b$  in  $G$ , the right cosets  $aH$  and  $bH$  (or the left cosets  $Ha$  and  $Hb$ ) are either identical or disjoint.

Final Answer: A

\*\*\*\*\*

Answer Option 3:

Statement 1: True. The right and left cosets ( $aH$  and  $Ha$ ) of a subgroup  $H$  in a group  $G$  have the same size. This is because the mappings  $x \rightarrow ax$  and  $x \rightarrow xa$  (from  $H$  to  $aH$  and  $Ha$  respectively) are bijective.

Statement 2: True. For any  $a$  and  $b$  in  $G$ , either  $aH = bH$  or  $aH$  and  $bH$  are disjoint. This is a fundamental property of cosets in group theory.

So, both statements are true. Final Answer: A

\*\*\*\*\*

Answer Option 4:

Statement 1 is true because if  $H$  is a subgroup of  $G$  and  $a$  belongs to  $G$ , then left coset  $aH$  and right coset  $Ha$  have the same number of elements as  $H$ , so  $|aH| = |Ha|$ .

Statement 2 is also true because in any group  $G$ , the left cosets  $aH$  and  $bH$  partition  $G$ . That is, every element of  $G$  is in exactly one such coset. Therefore, if  $aH$  and  $bH$  are not identical, they must be disjoint.

Final Answer: A. 'True, True'

\*\*\*\*\*

Answer Option 5:

Statement 1: True. It is known that for any subgroup  $H$  of a group  $G$  and any element  $a$  in  $G$ , the left coset  $aH$  and the right coset  $Ha$  have the same order. This is a fundamental property of cosets in group theory.

Statement 2: True. Again, this is a standard result in group theory. For any subgroup  $H$  of a group  $G$  and any elements  $a, b$  in  $G$ , the left coset  $aH$  and the right coset  $Hb$  are either identical or disjoint.

Final Answer: A. 'True, True'

\*\*\*\*\*

Answer Option 6:

Statement 1 is True: For any element  $a$  in  $G$ , the sets  $aH$  and  $Ha$  (known as left and right cosets, respectively) are of equal size, because they are simply the group  $H$  shifted by  $a$ .

Statement 2 is True: The left and right cosets of a subgroup  $H$  in  $G$  are either identical (when  $a=b$ ) or disjoint (when  $a \neq b$ ). This is because each coset represents a 'copy' of  $H$  in  $G$ , and these 'copies' do not overlap unless they are identical.

Final answer: A. 'True, True'

\*\*\*\*\*

Answer Option 7:

Statement 1: True. This is a property of subgroups in group theory. If  $H$  is a subgroup of  $G$  and  $a$  is an element in  $G$ , then the left coset  $aH$  (the set of elements obtained by multiplying  $a$  to each element in  $H$  from the left) has the same number of elements as the right coset  $Ha$  (the set of elements obtained by multiplying  $a$  to each element in  $H$  from the right).

Statement 2: True. This is also a property of subgroups in group theory. If  $H$  is a subgroup of  $G$  and  $a$  and  $b$  are elements in  $G$ , then the left coset  $aH$  and right coset  $Hb$  are either identical (if  $a$  and  $b$  are in the same coset) or disjoint (if  $a$  and  $b$  are in different cosets). They cannot partially overlap.

Final answer: A. 'True, True'

\*\*\*\*\*

Answer Option 8:

Statement 1 is true. If  $H$  is a subgroup of  $G$  and  $a$  belongs to  $G$ , then the right coset  $aH$  and the left coset  $Ha$  of  $H$  in  $G$  must have the same number of elements. This is a property of cosets in group theory.

Statement 2 is also true. For any subgroup  $H$  of  $G$  and any elements  $a$  and  $b$  in  $G$ , the right coset  $aH$  and the left coset  $Hb$  must either be the same set or have no elements in common. This is because a coset is a set of the form  $aH$  or  $Ha$ , and by definition, two cosets are either identical or disjoint.

So, both statements are true. Therefore, the correct answer is A. 'True, True'.

\*\*\*\*\*

Answer Option 9:

Statement 1 is true. The left and right cosets,  $aH$  and  $Ha$ , indeed have the same size for any group  $G$  and subgroup  $H$ .

Statement 2 is also true. For any elements  $a$  and  $b$  in  $G$ , the left coset  $aH$  and the right coset  $Hb$  are either identical (when  $a$  is in  $Hb$  or  $b$  is in  $aH$ ) or they are disjoint (they have no elements in common). This is a fundamental property of cosets in group theory.

So, the correct answer is A. 'True, True'.

\*\*\*\*\*

Question 12:

'If  $A = \{1, 2, 3\}$  then relation  $S = \{(1, 1), (2, 2)\}$  is', A. 'symmetric only', B. 'anti-symmetric only', C. 'both symmetric and anti-symmetric', D. 'an equivalence relation'

=====

Answer Option 1:

A relation  $S$  is symmetric if for every pair  $(a,b)$  in  $S$ , the pair  $(b,a)$  is also in  $S$ . In this case,  $(1,1)$  and  $(2,2)$  are indeed symmetric because changing the order in each pair does not result in a new pair.

A relation  $S$  is anti-symmetric if for every pair  $(a,b)$  in  $S$ , the pair  $(b,a)$  is not in  $S$  unless  $a = b$ . In this case,  $(1,1)$  and  $(2,2)$  are indeed anti-symmetric because changing the order in each pair does not result in a new pair since  $a = b$  in both pairs.

Therefore, the relation  $S$  is both symmetric and anti-symmetric. Final Answer: C.

=====

Answer Option 2:

A relation is symmetric if for every  $(a, b)$  in  $S$ ,  $(b, a)$  is also in  $S$ . Here  $(1, 1)$  and  $(2, 2)$  are already symmetric because swapping the elements doesn't change the pairs.

A relation is anti-symmetric if for every  $(a, b)$  in  $S$  where  $a \neq b$ ,  $(b, a)$  is not in  $S$ . Here, there is no  $(a, b)$  in  $S$  where  $a \neq b$ , so it's trivially anti-symmetric.

Therefore, the relation  $S$  is both symmetric and anti-symmetric. Final Answer: C

=====

Answer Option 3:

A relation  $R$  on a set  $A$  is said to be symmetric, if  $(a, b) \in R$  implies  $(b, a) \in R$ , for all  $a, b \in A$ . In this case,  $(1, 1) \in S$  and  $(1, 1) \in S$ , and  $(2, 2) \in S$  and  $(2, 2) \in S$ . Therefore,  $S$  is symmetric.

A relation  $R$  on a set  $A$  is said to be antisymmetric, if  $(a, b) \in R$  and  $(b, a) \in R$ , implies  $a = b$  for all  $a, b \in A$ . Here, for every ordered pair  $(a, b) \in S$ , there is also a pair  $(b, a) \in S$ , and  $a = b$ . So,  $S$  is also antisymmetric.

Therefore,  $S$  is both symmetric and antisymmetric. The final answer is C.

=====

Answer Option 4:

A relation is symmetric if for every  $(a, b)$  in the relation,  $(b, a)$  is also present. Here, for every  $(a, b)$  in  $S$ ,  $(b, a)$  is also present, so  $S$  is symmetric.

A relation is anti-symmetric if, for every  $(a, b)$  in the relation where  $a \neq b$ ,  $(b, a)$  is not present. In  $S$ , there is no pair  $(a, b)$  such that  $a \neq b$ , so  $S$  is anti-symmetric.

Therefore,  $S$  is both symmetric and anti-symmetric, so the answer is C. 'both symmetric and anti-symmetric'.

=====

Answer Option 5:

A relation  $R$  on a set  $A$  is called symmetric if for every  $(x, y)$  in  $R$ , there is a  $(y, x)$  in  $R$ . Given relation is symmetric because for every  $(x, y)$  in  $S$ , there is a  $(y, x)$  in  $S$ .

A relation  $R$  on a set  $A$  is called antisymmetric if and only if for any  $(a, b)$  in  $R$  where  $a \neq b$ ,  $(b, a)$  is not in  $R$ . Clearly, this is also true for the given relation as there are no  $(a, b)$  and  $(b, a)$  pairs where  $a \neq b$ .

Hence, the relation  $S$  on set  $A$  is both symmetric and anti-symmetric. Final Answer: C.

=====

Answer Option 6:

A relation  $S$  on a set  $A$  is said to be symmetric if  $(b, a) \in S$  whenever  $(a, b) \in S$ , for all  $a, b \in A$ . The given relation is symmetric because  $(1, 1)$  and  $(2, 2)$  both have  $(b, a)$  in  $S$ .

A relation  $S$  on a set  $A$  is said to be anti-symmetric if  $(b, a) \in S$  and  $(a, b) \in S$  only if  $a = b$ , for all  $a, b \in A$ . The given relation is anti-symmetric because  $(1, 1)$  and  $(2, 2)$  satisfy the condition, and there are no other elements in  $S$ .

So, the relation  $S$  is both symmetric and anti-symmetric.

Final answer: C

=====

Answer Option 7:

A relation is symmetric if whenever  $(a,b)$  is in the relation, then so is  $(b,a)$ . A relation is anti-symmetric if whenever  $(a,b)$  and  $(b,a)$  are in the relation, then  $a = b$ .

The given relation,  $\{(1, 1), (2, 2)\}$ , is both symmetric and anti-symmetric. For every pair  $(a, b)$  in the relation, the pair  $(b, a)$  is also in the relation, satisfying the definition of symmetric. Further, for every pair  $(a, b)$  and  $(b, a)$  in the relation,  $a = b$ , satisfying the definition of anti-symmetric.

Therefore, the answer is C. 'both symmetric and anti-symmetric'.

=====

Answer Option 8:

A relation  $R$  on a set  $A$  is called symmetric if  $(a, b) \in R$  implies  $(b, a) \in R$ . Here,  $(1, 1)$  and  $(2, 2)$  are both in  $S$ , and their reversed pairs  $(1, 1)$  and  $(2, 2)$  are also in  $S$ , so  $S$  is symmetric.

A relation  $R$  on a set  $A$  is called anti-symmetric if  $(a, b) \in R$  and  $(b, a) \in R$  implies  $a = b$ . Here, the only pairs in  $S$  are  $(1, 1)$  and  $(2, 2)$ , and in both cases  $a = b$ , so  $S$  is anti-symmetric.

Therefore,  $S$  is both symmetric and anti-symmetric. However, it isn't an equivalence relation because it doesn't satisfy reflexivity for all elements of  $A$  (for instance,  $(3, 3)$  isn't in  $S$ ). So, the answer is C. 'both symmetric and anti-symmetric' .

=====

Answer Option 9:

A relation  $R$  on a set  $A$  is called symmetric if  $(a, b) \in R$  implies that  $(b, a) \in R$  for all  $a, b \in A$ . In this case, for  $(1, 1)$  we do have  $(1, 1)$  and for  $(2, 2)$  we do have  $(2, 2)$  so it is symmetric.

A relation  $R$  on a set  $A$  is called antisymmetric if and only if for any  $a$  and  $b$  in  $A$ , whenever  $(a, b) \in R$  and  $(b, a) \in R$ , it must be the case that  $a = b$ . In this case, for  $(1, 1)$  we do have  $(1, 1)$  and for  $(2, 2)$  we do have  $(2, 2)$  so it is antisymmetric.

Hence, the relation  $S$  is both symmetric and antisymmetric. So, the answer is C. 'both symmetric and anti-symmetric'.

\*\*\*\*\*

Question 13:

'Find the order of the factor group  $(\mathbb{Z}_{11} \times \mathbb{Z}_{15}) / \langle (1, 1) \rangle$ , A. '1', B. '2', C. '5', D. '11'

=====

Answer Option 1:

The order of the factor group is the index of the subgroup in the original group. Since the subgroup is generated by  $\langle (1, 1) \rangle$ , all elements of the form  $(n, n)$  for integer  $n$  will belong to the subgroup. There are  $\gcd(11, 15) = 1$  element of this form. So the index of the subgroup, which is the order of the factor group, is  $(11 \cdot 15) / 1 = 165$ . The answer is not in options A, B, C, D.

\*\*\*\*\*

Answer Option 2:

The order of  $\mathbb{Z}_n$  is  $n$ , so the order of  $\mathbb{Z}_{11} \times \mathbb{Z}_{15}$  is  $11 \cdot 15 = 165$ . The order of  $\langle (1, 1) \rangle$  is the least common multiple of 11 and 15, which is 165. So the order of the quotient group is  $165 / 165 = 1$ . Final answer: A.

\*\*\*\*\*

Answer Option 3:

The order of  $\mathbb{Z}_{11} \times \mathbb{Z}_{15}$  is  $11 \cdot 15 = 165$ , and the order of the subgroup  $\langle (1, 1) \rangle$  is  $\text{lcm}(11, 15) = 165$ , so the order of the factor group  $(\mathbb{Z}_{11} \times \mathbb{Z}_{15}) / \langle (1, 1) \rangle$  is  $165 / 165 = 1$ . Final Answer: A

\*\*\*\*\*

Answer Option 4:

The order of the group  $\mathbb{Z}_{11} \times \mathbb{Z}_{15}$  is  $11 \cdot 15 = 165$ .

The order of the subgroup  $\langle (1, 1) \rangle$  is the least common multiple of 11 and 15, which is 165.

Then, the order of the factor group  $(\mathbb{Z}_{11} \times \mathbb{Z}_{15}) / \langle (1, 1) \rangle$  is  $165 / 165 = 1$ . Therefore, the correct answer is 1. Final Answer: A

\*\*\*\*\*

Answer Option 5:

The order of the group  $\mathbb{Z}_{11} \times \mathbb{Z}_{15}$  is  $11 \cdot 15 = 165$ . The order of the subgroup  $\langle (1, 1) \rangle$  is the least common multiple of 11 and 15, which is 165.

Therefore, the order of the factor group  $(\mathbb{Z}_{11} \times \mathbb{Z}_{15}) / \langle (1, 1) \rangle$  is  $165 / 165 = 1$ . Final Answer: A

\*\*\*\*\*

Answer Option 6:

The order of the group  $\mathbb{Z}_{11} \times \mathbb{Z}_{15}$  is equal to the product of the orders of  $\mathbb{Z}_{11}$  and  $\mathbb{Z}_{15}$ , which is  $11 \cdot 15 = 165$ .

The subgroup generated by  $(1, 1)$  contains all elements of the form  $(k, k)$ , where  $k \in \mathbb{Z}$ , modulo the orders of the respective groups. This gives us 11 unique elements, since that is the least common multiple of the orders of the two groups.

The order of a factor group  $G/H$  is equal to the order of  $G$  divided by the order of  $H$ . In this case, the order of the factor group is  $165 / 11 = 15$ . Final answer: D

\*\*\*\*\*

Answer Option 7:

The order of the factor group  $(\mathbb{Z}_{11} \times \mathbb{Z}_{15}) / \langle (1, 1) \rangle$  is equal to the index of  $\langle (1, 1) \rangle$  in  $\mathbb{Z}_{11} \times \mathbb{Z}_{15}$ . This index is equal to the least positive integer  $k$  such that  $k(1, 1) = (0, 0)$  in  $\mathbb{Z}_{11} \times \mathbb{Z}_{15}$ .

This means we need to find the least positive integer  $k$  such that  $k$  is a multiple of both 11 (the order of the group  $\mathbb{Z}_{11}$ ) and 15 (the order of the group  $\mathbb{Z}_{15}$ ).

The least common multiple of 11 and 15 is 165, so the order of the factor group  $(\mathbb{Z}_{11} \times \mathbb{Z}_{15}) / \langle (1, 1) \rangle$  is 165.

But since the options only go up to 11, it seems like there's been a mistake in the formulation of the problem. Among the given options, none of them is correct.

\*\*\*\*\*

Answer Option 8:

The order of the group  $\mathbb{Z}_{11} \times \mathbb{Z}_{15}$  is  $11 \cdot 15 = 165$ .

The subgroup generated by  $(1, 1)$  in  $\mathbb{Z}_{11} \times \mathbb{Z}_{15}$  is isomorphic to  $\mathbb{Z}_{\gcd(11, 15)} = \mathbb{Z}_1$ , so it has order 1.

The order of the factor group is the quotient of the order of the group by the order of the subgroup, so the order of the factor group is  $165 / 1 = 165$ .

Therefore, the order of the factor group  $(\mathbb{Z}_{11} \times \mathbb{Z}_{15}) / \langle (1, 1) \rangle$  is not given in the options A, B, C, or D.

\*\*\*\*\*

Answer Option 9:

A subgroup of  $\mathbb{Z}_m \times \mathbb{Z}_n$  of the form  $\langle (a, b) \rangle$  is isomorphic to  $\mathbb{Z}_{\gcd(m, a)} \times \mathbb{Z}_{\gcd(n, b)}$ .

Therefore, this problem is equivalent to finding the order of  $\mathbb{Z}_{11} \times \mathbb{Z}_{15} / \mathbb{Z}_{\gcd(11, 1)} \times \mathbb{Z}_{\gcd(15, 1)} = \mathbb{Z}_{11} \times \mathbb{Z}_{15} / \mathbb{Z}_1 \times \mathbb{Z}_1$ .

The order of the factor group is  $(\mathbb{Z}_{11} \times \mathbb{Z}_{15}) / \langle (1, 1) \rangle = (11 \cdot 15) / 1 = 165$ .

But since there is no option for '165', the problem seems to be incorrect. The provided options do not contain the correct answer.

\*\*\*\*\*

Question 14:

'The polynomial  $x^3 + 2x^2 + 2x + 1$  can be factored into linear factors in  $\mathbb{Z}_7[x]$ . Find this factorization.' A. ' $(x - 2)(x + 2)(x - 1)$ ', B. ' $(x + 1)(x + 4)(x - 2)$ ', C. ' $(x + 1)(x - 4)(x - 2)$ ', D. ' $(x - 1)(x - 4)(x - 2)$ '

=====

Answer Option 1:

We can factorize the polynomial by checking which values of  $x$  in  $\mathbb{Z}_7$  make the polynomial zero. These values of  $x$  will be the roots of the polynomial, which can be used in the factorization. Checking all possible values, we find that  $x=1$ ,  $x=3$ , and  $x=6$  are the roots of the polynomial. Hence, the factorization is  $(x-1)(x-3)(x-6)$ . However, in  $\mathbb{Z}_7$ , 3 is equivalent to -4 and 6 is equivalent to -1. So, the factorization becomes  $(x-1)(x+4)(x+1)$ .

Final answer: D

=====

Answer Option 2:

First, we find the roots of the cubic by plugging in the numbers 0, 1, 2, 3, 4, 5, and 6 in  $\mathbb{Z}_7$ . We find that the roots are 1, 3, and 6. Therefore, the polynomial factors as  $(x - 1)(x - 3)(x - 6)$  in  $\mathbb{Z}_7[x]$ . Now we convert this to the form given in the answer choices. We can write this as  $(x - 1)(x + 4)(x + 1)$ , which matches choice B. So the answer is  $\boxed{(x + 1)(x + 4)(x - 2)}$ . Final answer: B

=====

Answer Option 3:

We need to find the roots of the polynomial (which will be the factors) in  $\mathbb{Z}_7[x]$ , so we substitute  $x = 0, 1, 2, \dots, 6$  and find that the polynomial equals zero for  $x = 1, 4$ , and  $2$ . Thus, the linear factors are  $(x - 1)$ ,  $(x - 4)$ , and  $(x - 2)$ , so the answer is  $\boxed{(x - 1)(x - 4)(x - 2)}$ . Final answer: D

=====

Answer Option 4:

In  $\mathbb{Z}_7[x]$ , we only need to check the linear factors corresponding to the seven possible roots, namely 0, 1, 2, 3, 4, 5, and 6 (which are the same as -4, -3, -2, -1, 0, 1, and 2 in  $\mathbb{Z}_7$ ). Substituting these values in the polynomial, we find that the roots are 1, -2, and -4. Hence, the factorization is  $(x - 1)(x + 2)(x + 4)$ , which, after rearranging, becomes  $(x - 1)(x - 5)(x - 3)$ . Final Answer: D

=====

Answer Option 5:

We want to find the roots of this polynomial modulo 7, as these will give us the linear factors. So we need to solve  $x^3 + 2x^2 + 2x + 1 = 0 \pmod{7}$  for  $x$ . Checking each of the possible residues mod 7, we find that the roots are  $x = 1$ ,  $x = 2$ , and  $x = -4 = 3$ . Thus, the factorization is  $(x - 1)(x - 2)(x - 3)$ , which matches choice (C). The factors can be rearranged in any order, so the same factorization could also be written as  $(x - 2)(x - 1)(x - 3)$ ,  $(x - 2)(x - 3)(x - 1)$ , etc.

Final Answer: C

=====

Answer Option 6:

If a polynomial  $f(x)$  has a factor of  $(x - r)$  in  $\mathbb{Z}_7[x]$ , this means that  $f(r) \equiv 0 \pmod{7}$ . Checking the values from 0 to 6 in the polynomial, we find that  $f(1) \equiv 0 \pmod{7}$ ,  $f(2) \equiv 0 \pmod{7}$ , and  $f(4) \equiv 0 \pmod{7}$ . Thus, the linear factorization of the polynomial is  $\boxed{(x - 1)(x - 2)(x - 4)}$ . Final answer: D

=====

Answer Option 7:

First, we need to find the roots of the polynomial in the field  $\mathbb{Z}_7[x]$ . This can be done by plugging in each element of  $\mathbb{Z}_7$  (0, 1, 2, 3, 4, 5, 6) into the polynomial and checking if the result is 0.

The roots of the polynomial are  $x = 1$ ,  $x = 2$ , and  $x = 4$ .

Therefore, the factorization is  $(x - 1)(x - 2)(x - 4)$ . This is equivalent to  $(x + 6)(x + 5)(x + 3)$  in  $\mathbb{Z}_7[x]$  because -1 is equivalent to 6, -2 is equivalent to 5, and -4 is equivalent to 3 in  $\mathbb{Z}_7[x]$ .

So, the answer is  $(x - 1)(x - 2)(x - 4)$  which is option D. Final answer: D

=====

Answer Option 8:

If we plug in  $x=2$ , we obtain  $2^3 + 2 \cdot 2^2 + 2 \cdot 2 + 1 = 8 + 8 + 4 + 1 = 21 = 0 \pmod{7}$ . Therefore,  $x-2$  is a factor. We can use synthetic division to find the other factor:

\[

\begin{array}{c|ccc}

2 & 1 & 2 & 2 & 1 \\

& & 2 & 8 & 6 \\

\hline

& 1 & 4 & 3 & 0 \\

\end{array}

\]

We obtain  $x^2 + 4x + 3$ , which factors as  $(x+1)(x+2)$  (in  $\mathbb{Z}_7[x]$ ,  $-1 = 6$ , and  $-2 = 5$ ). Therefore, the factorization of the original polynomial in  $\mathbb{Z}_7[x]$  is  $(x-2)(x+1)(x+2)$

$\rightarrow \boxed{(x-2)(x-6)(x-5)}$ . Final Answer: B

=====

Answer Option 9:

We first need to find the roots of the polynomial in  $\mathbb{Z}_7$ . This can be done by substituting the numbers 0 to 6 into the polynomial and checking if the result is zero.

When  $x = 1$ , the polynomial becomes  $1 + 2 + 2 + 1 = 6 \pmod{7}$ .



When  $x = 2$ , the polynomial becomes  $8 + 8 + 4 + 1 = 21 \equiv 0 \pmod{7}$ .

When  $x = 3$ , the polynomial becomes  $27 + 18 + 6 + 1 = 52 \equiv 3 \pmod{7}$ .

When  $x = 4$ , the polynomial becomes  $64 + 32 + 8 + 1 = 105 \equiv 0 \pmod{7}$ .

When  $x = 5$ , the polynomial becomes  $125 + 50 + 10 + 1 = 186 \equiv 5 \pmod{7}$ .

When  $x = 6$ , the polynomial becomes  $216 + 72 + 12 + 1 = 301 \equiv 6 \pmod{7}$ .

So the roots of the polynomial in  $\mathbb{Z}_7$  are 2 and 4.

However, since we are working in  $\mathbb{Z}_7$ , where subtraction is the same as adding a number's additive inverse, the roots can also be represented as -2 and -4.

Therefore, the polynomial can be factored as  $(x - 2)(x - (-2))(x - 4) = (x - 2)(x + 2)(x - 4)$  or  $(x - 2)(x - 4)(x + 2)$ .

So, the correct answer is  $\boxed{\text{A) } (x - 2)(x + 2)(x - 4)}$ .

\*\*\*\*\*

Question 15:

'Find the maximum possible order for an element of  $S_n$  for  $n = 10$ .' A. '6', B. '12', C. '30', D. '105'

=====

Answer Option 1:

The order of an element of  $S_n$  is the least common multiple of the lengths of its cycles when written in disjoint cycle notation, and this number must divide  $n!$ . For  $n = 10$ , we can have cycles of lengths 2, 3, and 5, and so the maximum possible order is  $2^2 \cdot 3 \cdot 5 = 30$ . Final answer: C.

\*\*\*\*\*

Answer Option 2:

The cycle decomposition of an element of  $S_n$  gives a partition of  $n$  into positive integers. The order of the element is the least common multiple of the elements of the partition. The minimum of the least common multiple is thus maximized when the partition consists of numbers that are as large as possible and relatively prime. Hence, for  $n = 10$ , the partition  $(5, 2)$  or equivalently  $(3, 3, 2, 2)$  gives the maximum, which is  $5 \cdot 2 = 10$  or  $3 \cdot 2 = 6$ . Thus the maximum possible order is  $\boxed{10}$ . However, this option is not given in the list. The next maximum possible value is  $\boxed{6}$  which is given in option A. So, the answer is A.

\*\*\*\*\*

Answer Option 3:

The order of an element in  $S_n$  is the least common multiple of the lengths of the cycles in its cycle decomposition. To maximize the order, we want the lengths of the cycles to be pairwise relatively prime (so that the least common multiple is as large as possible). The ten numbers should be broken into cycles of lengths 5, 2, 2, 1, which have orders 5, 2, 2, 1 respectively. The maximum possible order is thus  $5 \cdot 2 \cdot 2 = \boxed{20}$ . But there is no option '10', so there must be a mistake in the choices.

\*\*\*\*\*

Answer Option 4:

In  $S_n$ , the order of an element is the least common multiple of the lengths of the cycles in its cycle decomposition. Since lcms are increased by using more distinct primes, we want the lengths of the cycles in the decomposition to be powers of distinct primes. The cycle lengths must add up to 10, so we need to partition 10 into a sum of powers of distinct primes. The best we can do is  $10 = 2 + 3 + 5$ , which gives an element of order  $\text{lcm}(2, 3, 5) = \boxed{30}$ . Final answer: C

\*\*\*\*\*

Answer Option 5:

The order of an element in the symmetric group  $S_n$  is the least common multiple of the lengths of its disjoint cycles. For  $n = 10$ , the lengths of the disjoint cycles can be 10, or 9 and 1, or 8 and 2, or 7 and 3, and so on, until 5 and 5. The largest least common multiple is achieved with 5 and 5, or 4, 3, 2, and 1, so the maximum possible order is  $\boxed{12}$ . Final Answer: B.

\*\*\*\*\*

Answer Option 6:

In the symmetric group  $S_n$ , the order of an element is the least common multiple of the sizes of its cycles. To maximize the order of an element in  $S_{10}$ , we want to use the integers from 1 to 10 to create cycle sizes that are as large as possible but also pairwise relatively prime (so that the least common multiple is as large as possible). The best we can do is to create cycles of lengths 7, 2, and 1 (the 1-cycle is necessary because we've used up all integers from 1 to 10). The least common multiple of 7, 2, and 1 is  $\boxed{14}$ , which is the maximum possible order for an element of  $S_{10}$ . Final Answer: B.

\*\*\*\*\*

Answer Option 7:

By the cycle decomposition, a permutation is a product of disjoint cycles. The order of a permutation is the least common multiple of the lengths of its cycles.

The factorization of a positive integer into a product of primes is unique (up to the order of the factors). Therefore, to build the positive integer with the largest number of factors, we use as many different primes as possible. The primes less than or equal to 10 are 2, 3, 5, and 7, which multiply to 210. We can't actually reach 210, because the sum of the lengths of the cycles is 10, but we can reach  $2 + 3 + 5 = 10$ ,

so the maximum possible order for an element of  $S_{10}$  is

$2^2 \cdot 3 \cdot 5 = 30$ .

The final answer is C. '30'.

\*\*\*\*\*

Answer Option 8:

By the definition of the symmetric group  $S_n$ , an element of  $S_n$  is a permutation of  $n$  objects. We can regard a permutation as a product of disjoint cycles, and the order of a permutation is the least common multiple of the lengths of these cycles. For example, the permutation  $(1, 2)(3, 4, 5)$  of  $S_5$  is of order  $\text{lcm}(2, 3) = 6$ .

The maximum order for an element of  $S_n$  is achieved by a permutation that is a product of disjoint cycles of lengths that are distinct primes, each raised to the greatest possible power. This maximizes the least common multiple of the cycle lengths.

For  $S_{10}$ , the primes less than or equal to 10 are 2, 3, 5, 7. However, we can only have cycles of length 7 if  $n \geq 7$ , so the maximum possible order for an element of  $S_{10}$  is  $\text{lcm}(2, 3, 5) = 30$ , which is achieved by a permutation that is a product of a 2-cycle, a 3-cycle, and a 5-cycle.

Final answer: C. '30'

\*\*\*\*\*

Answer Option 9:

The order of a permutation is the least common multiple of the lengths of its cycles. The least common multiple of a set of numbers cannot exceed their product. Hence the order of a permutation in  $S_{10}$  cannot exceed  $10!$ , but  $10!$  is divisible by all positive integers less than or equal to  $10$ , so in particular, it is divisible by all orders of elements of  $S_{10}$ .

We claim there exists a permutation in  $S_{10}$  of order  $30$ . Consider the permutation that sends  $1$  to  $2$ ,  $2$  to  $3$ ,  $3$  back to  $1$ ,  $4$  to  $5$ ,  $5$  back to  $4$ , and fixes all other elements. This permutation is a product of a  $3$ -cycle and a  $2$ -cycle, so its order is  $\text{lcm}(2,3) = 6$ .

For a permutation of order  $30$ ,  $30$  must be the least common multiple of the lengths of its cycles. The only way to write  $30$  as a product of distinct positive integers is  $30 = 2 \cdot 3 \cdot 5$ , so the permutation must consist of a  $2$ -cycle, a  $3$ -cycle, and a  $5$ -cycle. Consider the permutation that sends  $1$  to  $2$ ,  $2$  back to  $1$ ,  $3$  to  $4$ ,  $4$  to  $5$ ,  $5$  back to  $3$ ,  $6$  to  $7$ ,  $7$  to  $8$ ,  $8$  to  $9$ ,  $9$  to  $10$ ,  $10$  back to  $6$ , and fixes all other elements. This permutation is a product of a  $2$ -cycle, a  $3$ -cycle, and a  $5$ -cycle, so its order is  $\text{lcm}(2,3,5) = 30$ .

Therefore, the maximum possible order for an element of  $S_{10}$  is  $\boxed{30}$ . Final answer: C

\*\*\*\*\*

Question 16:

'Statement 1 |  $\mathbb{R}$  is a splitting field of some polynomial over  $\mathbb{Q}$ . Statement 2 | There is a field with 60 elements.', A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1: This is true.  $\mathbb{R}$ , the real numbers, is the splitting field of a real polynomial, for example, any linear polynomial.

Statement 2: This is false. The order of a finite field must be a power of a prime number, and 60 is not a power of a prime.

So, the answer is C. 'True, False'.

=====

Answer Option 2:

Statement 1: True. The real numbers are a splitting field of a polynomial over the rationals, such as  $x^2 + 1 = 0$ , which has solutions that are not rational but are real.

Statement 2: False. The number of elements in a finite field must be a prime power, and 60 is not a power of a prime.

Final Answer: C

=====

Answer Option 3:

Statement 1: True. The field of real numbers  $\mathbb{R}$  is a splitting field of a polynomial over  $\mathbb{Q}$ . For example, the polynomial  $x^2 - 2$  has roots  $\sqrt{2}$  and  $-\sqrt{2}$ , and  $\mathbb{R}$  is the smallest field containing  $\mathbb{Q}$  and these roots.

Statement 2: False. The order of a finite field must be a power of a prime number. Since 60 is not a power of a prime ( $60 = 2^2 \cdot 3 \cdot 5$ ), there does not exist a field with 60 elements.

Final Answer: C. 'True, False'

=====

Answer Option 4:

Statement 1 is True. The field of real numbers  $\mathbb{R}$  is the splitting field of the polynomial  $x^2 + 1$  over  $\mathbb{Q}$ .

Statement 2 is False. A finite field must have  $p^n$  elements, where  $p$  is a prime number and  $n$  is a natural number. Since 60 cannot be expressed in this form, there is no field with 60 elements.

So, the answer is  $\boxed{\text{(C) 'True, False'}}$ .

=====

Answer Option 5:

Statement 1: True. The field of real numbers  $\mathbb{R}$  is indeed a splitting field of some polynomial over  $\mathbb{Q}$ . For example, the polynomial  $x^2 + 1$  has roots in  $\mathbb{R}$  (namely,  $i$  and  $-i$ ) but not in  $\mathbb{Q}$ .

Statement 2: False. The number of elements in a finite field must be a power of a prime, and 60 is not a power of a prime. Therefore, there cannot be a field with exactly 60 elements.

Final answer: C. 'True, False'

=====

Answer Option 6:

Statement 1: True. The real numbers form a splitting field of, for instance, the polynomial  $x^2 + 1$  over  $\mathbb{Q}$ . This polynomial has roots  $i$  and  $-i$ , both of which are in  $\mathbb{R}$ .

Statement 2: False. In general, a finite field must have  $p^n$  elements, where  $p$  is a prime number and  $n$  is a positive integer. Since 60 is not a power of a prime (it's prime decomposition is  $2^2 \cdot 3 \cdot 5$ ), there cannot be a field with 60 elements.

Final Answer: C

=====

Answer Option 7:

Statement 1: The splitting field of a polynomial over  $\mathbb{Q}$  is a field extension of  $\mathbb{Q}$  which is a vector space over  $\mathbb{Q}$ . Since  $\mathbb{R}$  is an extension of  $\mathbb{Q}$  and is a vector space over  $\mathbb{Q}$ ,  $\mathbb{R}$  can be a splitting field of a polynomial over  $\mathbb{Q}$ . So, Statement 1 is True.

Statement 2: The order (number of elements) of a finite field must be a power of a prime number.  $60 = 2^2 \cdot 3 \cdot 5$  is not a power of a prime, so there cannot be a field with 60 elements. Statement 2 is false.

So, the final answer is C. 'True, False'

=====

Answer Option 8:

Statement 1: True. The field of real numbers  $\mathbb{R}$  is a splitting field of the polynomial  $x^2 + 1$  over  $\mathbb{Q}$ . (The splitting field is the smallest field extension of the base field over which a given polynomial splits into linear factors.)

Statement 2: False. A finite field must have  $p^n$  elements, where  $p$  is a prime number and  $n$  is a positive integer. 60 is not a power of a prime number.

Hence, the correct answer is C. 'True, False'.

=====

Answer Option 9:

Statement 1: True. The field of real numbers  $\mathbb{R}$  is a splitting field of many polynomials over  $\mathbb{Q}$ . For example, the polynomial  $x^2 - 2$  splits into  $(x - \sqrt{2})(x + \sqrt{2})$  in  $\mathbb{R}$ , so  $\mathbb{R}$  is a splitting field of  $x^2 - 2$  over  $\mathbb{Q}$ .

Statement 2: False. The number of elements in a finite field is always a power of a prime number, and  $60 = 2^2 \cdot 3 \cdot 5$  is not a power of a prime number. There is no finite field with 60 elements.

So, the correct answer is C. 'True, False'

=====



Question 17:

The inverse of  $-i$  in the multiplicative group,  $\{1, -1, i, -i\}$  is', A. '1', B. '-1', C. 'i', D. '-i'

=====

Answer Option 1:

The multiplicative inverse of a number  $a$  is a number  $b$  such that  $ab = 1$ . Therefore, since  $-i \cdot i = i^2 = -1$ , the multiplicative inverse of  $-i$  is  $\boxed{-i}$ . Final answer: D

\*\*\*\*\*

Answer Option 2:

The multiplicative inverse of a number is a number that, when multiplied with the original number, gives a product of 1. When we multiply  $-i$  by  $i$ , we get  $-i^2 = -(-1) = 1$ . Therefore, the multiplicative inverse of  $-i$  in the group  $\{1, -1, i, -i\}$  is 'i'. Final Answer: C

\*\*\*\*\*

Answer Option 3:

The multiplicative inverse of a number is a number such that when the two are multiplied together, the result is 1. Given that  $-i$  is the number we're trying to find the inverse for, we can see that the product of  $-i$  and  $i$  equals 1. Therefore, the multiplicative inverse of  $-i$  in this set is 'i'. Final answer: C.

\*\*\*\*\*

Answer Option 4:

The multiplicative inverse of a number is a number that, when multiplied by the original number, yields 1. So we need to find a number in the set  $\{1, -1, i, -i\}$  that, when multiplied by  $-i$ , gives 1. Checking the possibilities, we find that  $-i \cdot i = 1$ . So, the multiplicative inverse of  $-i$  is  $i$ . Final answer: D.

\*\*\*\*\*

Answer Option 5:

The multiplicative inverse of a number  $x$  is a number such that when  $x$  is multiplied by its inverse, the product is 1. We can find the multiplicative inverse of  $-i$  by checking each option:

A.  $-i \cdot 1 = -i$

B.  $-i \cdot -1 = i$

C.  $-i \cdot i = -1$

D.  $-i \cdot -i = 1$

So, the inverse of  $-i$  in the multiplicative group  $\{1, -1, i, -i\}$  is ' $i$ '. Final Answer: D

\*\*\*\*\*

Answer Option 6:

The multiplicative inverse of a number is the number which, when multiplied by the original number, yields 1. In this case, we're looking for the inverse of  $-i$  in the group  $\{1, -1, i, -i\}$ . We know that  $i \cdot i = -1$ , so  $-i \cdot i = 1$ . Therefore, the inverse of  $-i$  is  $i$ . So, the answer is D. ' $i$ '.

\*\*\*\*\*

Answer Option 7:

The inverse of a number  $a$  in a multiplicative group is a number  $b$  such that  $a \cdot b = 1$ . Here, we have  $(-i) \cdot i = i^2 = -1$ ,  $(-i) \cdot (-1) = i$ ,  $(-i) \cdot 1 = -i$  and  $(-i) \cdot (-i) = i^2 = 1$ . So the inverse of  $-i$  in this group is  $\boxed{i}$ . Final Answer: C

\*\*\*\*\*

Answer Option 8:

The multiplicative inverse of a number is defined as a number which when multiplied by the original number gives 1. So, we need to find a number in the set  $\{1, -1, i, -i\}$  that gives 1 when multiplied by  $-i$ .

$-i \cdot 1 = -i$ ,  $-i \cdot -1 = i$ ,  $-i \cdot i = -1$  and  $-i \cdot -i = 1$ .

So, the inverse of  $-i$  in the multiplicative group,  $\{1, -1, i, -i\}$  is  $i$ . Final Answer: D

\*\*\*\*\*

Answer Option 9:

The multiplicative inverse of a number is the number which when multiplied to the original number gives the product as 1. So, we need to find a number in the group  $\{1, -1, i, -i\}$  which when multiplied to  $-i$  gives the product as 1.

If we multiply  $-i$  with  $-i$ , the result is  $-i \cdot -i = (-1) \cdot (i^2) = (-1) \cdot (-1) = 1$ .

So, the inverse of  $-i$  in the multiplicative group,  $\{1, -1, i, -i\}$  is  $-i$ .

Final answer: D

\*\*\*\*\*

Question 18:

'Compute the product in the given ring.  $(2,3)(3,5)$  in  $\mathbb{Z}_5 \times \mathbb{Z}_9$ '. A.  $(1,1)$ , B.  $(3,1)$ , C.  $(1,6)$ , D.  $(3,6)$

=====

Answer Option 1:

The product  $(2,3)(3,5)$  in the ring  $\mathbb{Z}_5 \times \mathbb{Z}_9$  is computed as  $(2 \cdot 3 \bmod 5, 3 \cdot 5 \bmod 9) = (6 \bmod 5, 15 \bmod 9) = (1, 6)$ . So, the answer is C.  $(1,6)$ .

\*\*\*\*\*

Answer Option 2:

In the ring  $\mathbb{Z}_5 \times \mathbb{Z}_9$ , the product of two ordered pairs is defined as the product of their components. Therefore,

$$(2,3)(3,5) = (2 \cdot 3 \bmod 5, 3 \cdot 5 \bmod 9) = (6 \bmod 5, 15 \bmod 9) = (1, 6).$$

So, the product is  $\boxed{(1,6)}$ . Final answer: C.

\*\*\*\*\*

Answer Option 3:

In the ring  $\mathbb{Z}_5 \times \mathbb{Z}_9$ , the product of two elements is defined as the product of their components in each ring. So, we have  $(2, 3) \cdot (3, 5) = (2 \cdot 3 \bmod 5, 3 \cdot 5 \bmod 9) = (6 \bmod 5, 15 \bmod 9) = (1, 6)$ .

The answer is  $\boxed{(1,6)}$  or C.

\*\*\*\*\*

Answer Option 4:

In the product  $(2,3)(3,5)$  in  $\mathbb{Z}_5 \times \mathbb{Z}_9$ , we multiply the first components together modulo 5 and the second components together modulo 9. Thus, we have  $(2 \cdot 3 \bmod 5, 3 \cdot 5 \bmod 9) = (6 \bmod 5, 15 \bmod 9) = \boxed{(1,6)}$ . Final answer: C

\*\*\*\*\*

Answer Option 5:

We compute the product componentwise. In  $\mathbb{Z}_5$ , we have  $2 \cdot 3 = 6 \equiv 1 \pmod{5}$ . In  $\mathbb{Z}_9$ , we have  $3 \cdot 5 = 15 \equiv 6 \pmod{9}$ . Therefore,  $(2,3) \cdot (3,5) = (1,6)$  in  $\mathbb{Z}_5 \times \mathbb{Z}_9$ . Final Answer: C.

\*\*\*\*\*

Answer Option 6:

In the ring  $\mathbb{Z}_n$ , we compute as usual, but then take the remainder when divided by  $n$ . This is often described by saying we "add (or multiply) mod  $n$ ". So, in the ring  $\mathbb{Z}_5 \times \mathbb{Z}_9$ , we add and multiply the first components modulo 5 and the second components modulo 9.

$$\text{Thus, } (2,3)(3,5) \text{ in } \mathbb{Z}_5 \times \mathbb{Z}_9 \text{ is } (2 \cdot 3 \bmod 5, 3 \cdot 5 \bmod 9) = (6 \bmod 5, 15 \bmod 9) = (1, 6).$$

So, the final answer is C.  $(1,6)$ .

\*\*\*\*\*

Answer Option 7:

In the ring  $\mathbb{Z}_5 \times \mathbb{Z}_9$ , the product of two elements  $(a,b)$  and  $(c,d)$  is given by  $(ac \bmod 5, bd \bmod 9)$ . So, the product of  $(2,3)$  and  $(3,5)$  is  $((2 \cdot 3) \bmod 5, (3 \cdot 5) \bmod 9) = (6 \bmod 5, 15 \bmod 9) = (1,6)$ . Therefore, the correct answer is C.  $(1,6)$

\*\*\*\*\*

Answer Option 8:

In the ring  $\mathbb{Z}_n$ , multiplication is done modulo  $n$ . So in  $\mathbb{Z}_5 \times \mathbb{Z}_9$ , the multiplication is done component-wise modulo 5 and 9 respectively. Therefore,  $(2,3)(3,5) = (2 \cdot 3 \bmod 5, 3 \cdot 5 \bmod 9) = (6 \bmod 5, 15 \bmod 9) = (1,6)$ . So, the product is  $\boxed{(1,6)}$ . Final answer: C.

\*\*\*\*\*

Answer Option 9:

In the direct product ring  $\mathbb{Z}_5 \times \mathbb{Z}_9$ , we define multiplication componentwise. Therefore,  $(2, 3) \cdot (3, 5) = (2 \cdot 3 \bmod 5, 3 \cdot 5 \bmod 9) = (6 \bmod 5, 15 \bmod 9) = (1, 6)$ . However, we have to take these products modulo 5 and 9, respectively, because of the ring we're in. So we get  $(6 \bmod 5, 15 \bmod 9) = (1, 6)$ . Hence, the product is  $\boxed{(1, 6)}$ . Final Answer: C

\*\*\*\*\*

Question 19:

'The set of all real numbers under the usual multiplication operation is not a group since', A. 'multiplication is not a binary operation', B. 'multiplication is not associative', C. 'identity element does not exist', D. 'zero has no inverse'

=====

Answer Option 1:

D. 'zero has no inverse'

\*\*\*\*\*

Answer Option 2:

D. 'zero has no inverse'

\*\*\*\*\*

Answer Option 3:

D. 'zero has no inverse'

\*\*\*\*\*

Answer Option 4:

D. 'zero has no inverse'

\*\*\*\*\*

Answer Option 5:

D. 'zero has no inverse'

\*\*\*\*\*

Answer Option 6:

D. 'zero has no inverse'

\*\*\*\*\*

Answer Option 7:

D. 'zero has no inverse'

\*\*\*\*\*

Answer Option 8:

The set of real numbers under multiplication does indeed form a binary operation and multiplication is associative. Also, the identity element does exist (which is 1). However, zero, which is included in the set of real numbers, does not have a multiplicative inverse (as no number multiplied by zero gives the identity, 1). Hence, the set of all real numbers under multiplication is not a group due to the absence of the multiplicative inverse for zero. Therefore, the correct answer is D. 'zero has no inverse'.

\*\*\*\*\*

Answer Option 9:

For the set of all real numbers to be a group under the operation of multiplication, it must satisfy four conditions:

1. The operation (in this case, multiplication) must be well-defined and closed. That is, for any two elements in the set, their product is also in the set. This is true for the set of all real numbers.
2. The operation must be associative. That is, for any three elements in the set, their product is the same regardless of how they are grouped. This is also true for the set of all real numbers.
3. There must be an identity element in the set. That is, there should be a number in the set such that, when any number in the set is multiplied by this number, the original number is unchanged. For multiplication, this number is 1, which is included in the set of all real numbers.
4. Every element in the set must have an inverse. That is, for every number in the set, there should be a number such that, when the two numbers are multiplied together, the result is the identity element.

However, for the zero in the set of all real numbers, there is no number you can multiply it by to get 1. Therefore, the set of all real numbers under the usual multiplication operation is not a group because 'zero has no inverse'. Final answer: D.

\*\*\*\*\*



Question 20:

'Statement 1| Every group of order  $p^2$  where  $p$  is prime is Abelian. Statement 2 | For a fixed prime  $p$  a Sylow  $p$ -subgroup of a group  $G$  is a normal subgroup of  $G$  if and only if it is the only Sylow  $p$ -subgroup of  $G$ .' A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1 is True. Every group of order  $p^2$  where  $p$  is a prime number is indeed Abelian. This is a well-known result in group theory.

Statement 2 is also True. By the Sylow theorems, if a group has exactly one Sylow  $p$ -subgroup, then it is normal in the group. So if a Sylow  $p$ -subgroup of a group  $G$  is normal, it must be the only one.

Therefore, the correct answer is A. 'True, True'.

\*\*\*\*\*

Answer Option 2:

Statement 1 is true. Every group of order  $p^2$  where  $p$  is a prime number is Abelian.

Statement 2 is also true. By the Sylow theorems, a Sylow  $p$ -subgroup of a group  $G$  is normal if and only if it is the only Sylow  $p$ -subgroup of  $G$ .

So, the correct answer is  $\boxed{\text{A. 'True, True'}}$ .

\*\*\*\*\*

Answer Option 3:

Statement 1 is True. Every group of order  $p^2$  where  $p$  is prime is indeed Abelian.

Statement 2 is also True. This is the Sylow theorem which states that a Sylow  $p$ -subgroup of a group  $G$  is a normal subgroup of  $G$  if and only if it is the only Sylow  $p$ -subgroup of  $G$ .

So, the correct answer is A. 'True, True'.

\*\*\*\*\*

Answer Option 4:

Statement 1 is true. All groups of order  $p^2$  where  $p$  is a prime number are indeed Abelian, which means that the group operation is commutative.

Statement 2 is also true. The Sylow theorems in group theory state that for a given prime number  $p$ , a Sylow  $p$ -subgroup of a group  $G$  is a normal subgroup if and only if it is the only Sylow  $p$ -subgroup of  $G$ .

Therefore, the correct answer is  $\boxed{\text{A. 'True, True'}}$ .

\*\*\*\*\*

Answer Option 5:

Statement 1 is true. Every group of order  $p^2$  where  $p$  is prime is indeed Abelian. This can be proven by using the class equation or using the fact that any group of order  $p^2$  is either  $\mathbb{Z}_{p^2}$  or  $\mathbb{Z}_p \times \mathbb{Z}_p$  both of which are abelian.

Statement 2 is also true. For a fixed prime  $p$ , a Sylow  $p$ -subgroup of a group  $G$  is a normal subgroup of  $G$  if and only if it is the only Sylow  $p$ -subgroup of  $G$ . This is a standard result in group theory, which follows from the Sylow theorems.

Thus, the answer is  $\boxed{\text{'True, True'}}$  or A.

\*\*\*\*\*

Answer Option 6:

Statement 1: Every group of order  $p^2$  where  $p$  is prime is Abelian. This statement is true. This is a result in group theory which says that every group of order  $p^n$  where  $p$  is a prime number and  $n$  is a positive integer is Abelian if and only if  $n \leq 2$ .

Statement 2: For a fixed prime  $p$ , a Sylow  $p$ -subgroup of a group  $G$  is a normal subgroup of  $G$  if and only if it is the only Sylow  $p$ -subgroup of  $G$ . This statement is also true. This is a result of the Sylow theorems in group theory.

So, both statements are True. Final Answer: A

\*\*\*\*\*

Answer Option 7:

Statement 1 is True. Every group of order  $p^2$  where  $p$  is a prime number is Abelian. This is a result of the Fundamental Theorem of Finite Abelian Groups.

Statement 2 is also True. This is a well-known result from Sylow theory which states that for a fixed prime  $p$ , a Sylow  $p$ -subgroup of a group  $G$  is a normal subgroup of  $G$  if and only if it is the only Sylow  $p$ -subgroup of  $G$ . This is because any two Sylow  $p$ -subgroups of  $G$  are conjugate in  $G$ , so if there's only one, it must be normal.

Therefore, the answer is A. 'True, True'.

\*\*\*\*\*

Answer Option 8:

Statement 1 is true. Every group of order  $p^2$  where  $p$  is prime is indeed Abelian. This is because any group of order  $p^2$  is either isomorphic to  $\mathbb{Z}_{p^2}$  or  $\mathbb{Z}_p \times \mathbb{Z}_p$ , both of which are Abelian.

Statement 2 is also true. Indeed, for a fixed prime  $p$ , a Sylow  $p$ -subgroup  $P$  of a group  $G$  is a normal subgroup of  $G$  if and only if it is the only Sylow  $p$ -subgroup of  $G$ . This follows directly from one of the Sylow theorems, which states that all Sylow  $p$ -subgroups of  $G$  are conjugate to each other. Thus, if  $P$  is the only Sylow  $p$ -subgroup, then it is normal in  $G$ .

So, both statements are true. Final answer: A.

\*\*\*\*\*

Answer Option 9:

Statement 1 is indeed true. Every group of order  $p^2$  is isomorphic to either  $\mathbb{Z}_{p^2}$  or  $\mathbb{Z}_p \times \mathbb{Z}_p$ . Both  $\mathbb{Z}_{p^2}$  and  $\mathbb{Z}_p \times \mathbb{Z}_p$  are abelian groups, therefore so is every group of order  $p^2$ .

Statement 2 is also true. In group theory, a Sylow  $p$ -subgroup of a group is a maximal  $p$ -subgroup of the group. If a group has exactly one Sylow  $p$ -subgroup, then that subgroup is normal. Conversely, if a Sylow  $p$ -subgroup is normal in the group, then it is the only Sylow  $p$ -subgroup.

So the final answer is  $\boxed{A}$  'True, True'.

\*\*\*\*\*

Question 21:

'Statement 1 | For finite groups  $G$  and  $H$ ,  $|G + H| = |G||H|$ . ( $G + H$  is the internal direct product.) Statement 2 | If  $r$  divides  $m$  and  $s$  divides  $n$  then  $Z_m + Z_n$  has a subgroup isomorphic to  $Z_r + Z_s$ .' A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1 is true. The internal direct product of two groups  $G$  and  $H$ , denoted  $G + H$ , is indeed the same size as the product of the sizes of  $G$  and  $H$ .

Statement 2 is false. The presence of a subgroup isomorphic to  $Z_r + Z_s$  in  $Z_m + Z_n$  does not necessarily depend on whether  $r$  divides  $m$  and  $s$  divides  $n$ .

So, the final answer is C. 'True, False'

\*\*\*\*\*

Answer Option 2:

Statement 1 is true: For finite groups  $G$  and  $H$ , the size of the direct product group  $G + H$  is equal to the product of the sizes of  $G$  and  $H$ . This is a basic result in group theory.

Statement 2 is also true: Given that  $r$  divides  $m$  and  $s$  divides  $n$ ,  $Z_m$  and  $Z_n$  each have subgroups isomorphic to  $Z_r$  and  $Z_s$ , respectively. The direct product of these subgroups is isomorphic to  $Z_r + Z_s$ , and can be considered a subgroup of  $Z_m + Z_n$ .

Final Answer: A. 'True, True'

\*\*\*\*\*

Answer Option 3:

Statement 1 is False because for finite groups  $G$  and  $H$ ,  $|G + H| = |G||H|$  only when  $G$  and  $H$  are disjoint. If  $G$  and  $H$  are not disjoint (for example, they share common elements), then  $|G + H|$  would be less than  $|G||H|$  because the common elements would be counted twice.

Statement 2 is True because if  $r$  divides  $m$  and  $s$  divides  $n$ , then  $Z_m$  and  $Z_n$  would certainly have subgroups isomorphic to  $Z_r$  and  $Z_s$  respectively. And the direct sum of these two subgroups is a subgroup of  $Z_m + Z_n$  which is isomorphic to  $Z_r + Z_s$ .

So the correct answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 4:

Statement 1 | For finite groups  $G$  and  $H$ ,  $|G + H| = |G||H|$ . ( $G + H$  is the internal direct product.) - True.

The internal direct product of two groups is the Cartesian product of the groups, so the size of the result is the product of the sizes of the groups.

Statement 2 | If  $r$  divides  $m$  and  $s$  divides  $n$  then  $Z_m + Z_n$  has a subgroup isomorphic to  $Z_r + Z_s$ . - False.

The statement would be true if it was about external direct product (denoted usually as  $Z_m \times Z_n$ ), not the internal direct product (denoted as  $Z_m + Z_n$ ).

So, the correct answer is C. 'True, False'.

\*\*\*\*\*

Answer Option 5:

Statement 1 is true. In group theory, the direct product (denoted  $G + H$  in this case) of two groups  $G$  and  $H$  is a group whose elements are ordered pairs from  $G$  and  $H$ , and whose group operation is defined componentwise. The order (or size) of  $G + H$  is then the product of the orders of  $G$  and  $H$ .

Statement 2 is false. The statement is talking about the direct sum  $Z_m + Z_n$ , which is a group formed from the integers modulo  $m$  and  $n$ . If  $r$  divides  $m$  and  $s$  divides  $n$ , there is not necessarily a subgroup of  $Z_m + Z_n$  isomorphic to  $Z_r + Z_s$ . For example, consider  $Z_4 + Z_6$  and  $r = s = 2$ .  $Z_2 + Z_2$  does not appear as a subgroup of  $Z_4 + Z_6$ .

Final Answer: C

\*\*\*\*\*

Answer Option 6:

Statement 1: True. The order of a group is the number of its elements. The internal direct product of two groups is a group whose elements are pairs of elements from the two groups and whose operation is componentwise. Thus, the order of the direct product of two finite groups  $G$  and  $H$  is  $|G||H|$ .

Statement 2: False. This statement isn't true in the general case. For example, let  $r=2$ ,  $m=4$ ,  $s=3$ , and  $n=6$ . Then  $Z_m = Z_4$  and  $Z_n = Z_6$ , both have  $Z_2$  as a subgroup, but  $Z_4 + Z_6 = Z_{24}$ , which does not have a subgroup isomorphic to  $Z_2 + Z_2 = Z_4$ .

So the correct answer is C. 'True, False'

\*\*\*\*\*

Answer Option 7:

Statement 1 is false. The order of the internal direct product  $G + H$  is not  $|G||H|$ , but rather the least common multiple of  $|G|$  and  $|H|$ , assuming that  $G$  and  $H$  are finite and that  $G \cap H$  is the trivial group.

Statement 2 is also false. For instance, consider  $m = 12$ ,  $n = 8$ ,  $r = 4$ , and  $s = 2$ . The group  $Z_{12} + Z_8$  is not isomorphic to  $Z_4 + Z_2$ .

So, the correct answer is B. 'False, False'.

\*\*\*\*\*

Answer Option 8:

Statement 1 | For finite groups  $G$  and  $H$ ,  $|G + H| = |G||H|$ . ( $G + H$  is the internal direct product.)

True. The internal direct product  $G \times H$  is the product of the orders of the groups  $G$  and  $H$ .

Statement 2 | If  $r$  divides  $m$  and  $s$  divides  $n$  then  $Z_m + Z_n$  has a subgroup isomorphic to  $Z_r + Z_s$ .

True. This is true due to the isomorphism theorems. If  $r|m$  and  $s|n$ , then  $Z_m$  has a subgroup isomorphic to  $Z_r$  and  $Z_n$  has a subgroup isomorphic to  $Z_s$ . By the definition of an internal direct product,  $Z_m + Z_n$  has a subgroup isomorphic to  $Z_r + Z_s$ .

Final Answer: A

\*\*\*\*\*

Answer Option 9:

Statement 1: This statement is true. If  $G$  and  $H$  are finite groups, then the order of their internal direct product (denoted here as  $G + H$ ) is indeed equal to the product of their individual orders. The internal direct product of two groups can be thought of as a "combination" of the two groups that preserves all of their structures.

Statement 2: This statement is false. The statement asserts that for any divisors  $r$  of  $m$  and  $s$  of  $n$ , the group  $Z_m + Z_n$  has a subgroup isomorphic to  $Z_r + Z_s$ . This is not true in general. For example, consider the case when  $m = n = 4$ ,  $r = s = 2$ . The group  $Z_4 + Z_4$  does not have a subgroup isomorphic to  $Z_2 + Z_2$ .

So the final answer is C. 'True, False'.

\*\*\*\*\*

Question 22:

'Find the sum of the given polynomials in the given polynomial ring.  $f(x) = 4x - 5$ ,  $g(x) = 2x^2 - 4x + 2$  in  $\mathbb{Z}_8[x]$ .' A. ' $2x^2 + 5$ ', B. ' $6x^2 + 4x + 6$ ', C. ' $0$ ', D. ' $x^2 + 1$ '

=====

Answer Option 1:

Adding the two polynomials gives  $h(x) = 2x^2 - 4x + 4x + 4x - 5 = 2x^2 - 5 \pmod{8}$ . However, in the ring  $\mathbb{Z}_8$ , we can replace -5 with 3, so the final answer is  $h(x) = 2x^2 + 3$ . This is not among the choices, so there seems to be a mistake in the question.

\*\*\*\*\*

Answer Option 2:

In  $\mathbb{Z}_8[x]$ , we simply add the coefficients for each term of the same degree, performing the operation modulo 8 if necessary.

Thus,  $f(x) + g(x) = 4x - 5 + 2x^2 - 4x + 2 = 2x^2 + 7$  in  $\mathbb{Z}_8[x]$ .

However, since we are working in  $\mathbb{Z}_8$ , -1 is equivalent to 7. So, the correct answer is :  $2x^2 - x - 1$ .

This option is not available in the options provided. The question may be incorrect.

\*\*\*\*\*

Answer Option 3:

The polynomial ring  $\mathbb{Z}_8[x]$  means the coefficients of the polynomials are integers modulo 8. Addition of polynomials is done term-by-term. Adding the given polynomials gives  $(4x - 5) + (2x^2 - 4x + 2) = 2x^2 + 4x - 5 + 2 = 2x^2$ . However, since we are working in  $\mathbb{Z}_8[x]$ , we reduce -5 + 2 modulo 8 to get -3 which is equivalent to 5 in  $\mathbb{Z}_8$ . Hence the sum of the polynomials is  $2x^2 + 5$ . Final answer: A

\*\*\*\*\*

Answer Option 4:

In the polynomial ring  $\mathbb{Z}_8[x]$ , all arithmetic operations are done mod 8. So we just add the polynomials term by term. The sum is  $2x^2 - 4x + 4x - 5 + 2 = 2x^2 - 3$ . However, we need to convert -3 into a representation from 0 to 7.  $-3 \pmod{8} = 5$ , so the final sum is  $2x^2 + 5$ . Final Answer: A

\*\*\*\*\*

Answer Option 5:

In the polynomial ring  $\mathbb{Z}_8[x]$ , all arithmetic is performed modulo 8. Therefore, when we add the polynomials  $f(x)$  and  $g(x)$ , we get:

$f(x) + g(x) = (4x - 5) + (2x^2 - 4x + 2) = 2x^2 + 4x + 6$ .

But in  $\mathbb{Z}_8[x]$ , we perform arithmetic modulo 8, so we reduce each coefficient modulo 8. The coefficients 2, 4, and 6 are already between 0 and 7, so they are unchanged. Therefore, the sum is  $2x^2 + 4x + 6$ .

Final answer: B.

\*\*\*\*\*

Answer Option 6:

The sum of two polynomials is found by adding their corresponding coefficients. Therefore,  $f(x) + g(x) = 4x - 5 + 2x^2 - 4x + 2 = 2x^2 + 2 \pmod{8} = 2x^2$ . However, in the ring  $\mathbb{Z}_8[x]$ ,  $-5 \equiv 3 \pmod{8}$  and  $2 \equiv 2 \pmod{8}$ . So the sum is  $2x^2 + 3$ . Final Answer: A

\*\*\*\*\*

Answer Option 7:

In the polynomial ring  $\mathbb{Z}_8[x]$ , we add the polynomials as usual but then reduce the coefficients modulo 8.

Thus,  $f(x) + g(x) = (4x - 5) + (2x^2 - 4x + 2) = 2x^2 + 4x - 5 + 2 = 2x^2 + 4x - 3 = 2x^2 - 4$ .

Then reducing the coefficients modulo 8, we get  $f(x) + g(x) = 2x^2 + 4 = 2x^2 - 4 = 2x^2 + 4$  in  $\mathbb{Z}_8[x]$ .

Hence, the correct final answer is A. ' $2x^2 + 5$ '.

\*\*\*\*\*

Answer Option 8:

The polynomial ring  $\mathbb{Z}_8[x]$  means that all our operations are done modulo 8. We add the polynomials  $f(x)$  and  $g(x)$  term by term. There is no  $x^2$  term in  $f(x)$ , so the  $x^2$  term in the sum is just the  $x^2$  term in  $g(x)$ , which is  $2x^2$ . The  $x$  term in the sum is the sum of the  $x$  terms,  $4x - 4x = 0$ . The constant term in the sum is the sum of the constants,  $-5 + 2 = -3$ . However, since we're working in  $\mathbb{Z}_8[x]$ , we know -3 is equivalent to 5 (since  $-3 + 8 = 5$ ). Therefore, our final sum is  $2x^2 + 0 + 5$ , or  $2x^2 + 5$ . Final Answer: A

\*\*\*\*\*

Answer Option 9:

In the ring  $\mathbb{Z}_8[x]$ , we perform addition modulo 8. So, we just add the corresponding coefficients of the polynomials:

$f(x) + g(x) = (4x - 5) + (2x^2 - 4x + 2) = 2x^2 + 6x + 6$ .

This result seems to not be in the options. However, in  $\mathbb{Z}_8$ , we know that  $6 \equiv -2 \pmod{8}$ . So, we can rewrite the result as:

$f(x) + g(x) = 2x^2 - 2x - 2$ .

This result is also not in the options. However, we can again use the properties of  $\mathbb{Z}_8$  to simplify further.

In  $\mathbb{Z}_8$ , we have:

$-2 \equiv 6 \pmod{8}$ ,

$-2x \equiv 6x \pmod{8}$ .

So the polynomial can be simplified to:

$f(x) + g(x) = 2x^2 + 6x + 6$ .

In  $\mathbb{Z}_8[x]$ , this is equivalent to the option B.  $'6x^2 + 4x + 6'$  because  $6 \equiv -2 \pmod{8}$ . So the final answer is B.  $'6x^2 + 4x + 6'$ .

\*\*\*\*\*

Question 23:

'Statement 1 | Any set of two vectors in  $\mathbb{R}^2$  is linearly independent. Statement 2 | If  $V = \text{span}\{v_1, \dots, v_k\}$  and  $\{v_1, \dots, v_k\}$  are linearly independent, then  $\dim(V) = k$ '. A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1 is false. A set of two vectors in  $\mathbb{R}^2$  can be linearly dependent if the vectors are multiples of each other.

Statement 2 is true. By definition, if  $k$  vectors are linearly independent and span the space  $V$ , then the dimension of  $V$  is indeed  $k$ .

Therefore, the correct answer would be D. 'False, True'.

\*\*\*\*\*

Answer Option 2:

Statement 1 is False. Two vectors in  $\mathbb{R}^2$  can be linearly dependent if one is a multiple of the other.

Statement 2 is True. The dimension of a vector space is the maximum number of linearly independent vectors in the space. If  $V$  is the span of a set of  $k$  linearly independent vectors, then there are  $k$  directions in which we can move, so the dimension of  $V$  is indeed  $k$ .

Final answer: D. 'False, True'

\*\*\*\*\*

Answer Option 3:

Statement 1 is False. Counter-example: The vectors  $\{v_1, v_2\} = \{(1, 0), (2, 0)\}$  are linearly dependent because  $v_2 = 2v_1$ .

Statement 2 is True. The dimension of a vector space is the maximum number of linearly independent vectors, and since  $\{v_1, \dots, v_k\}$  are given to be linearly independent,  $\dim(V) = k$ .

So, the correct answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 4:

Statement 1 is false. A set of two vectors in  $\mathbb{R}^2$  is not necessarily linearly independent. For instance, consider the vectors  $(1,0)$  and  $(2,0)$ . The second is just 2 times the first, so these vectors are linearly dependent.

Statement 2 is true. If  $V$  is the span of  $v_1, \dots, v_k$  and these vectors are all linearly independent, then by definition, the dimension of  $V$  is equal to the number of vectors in the basis, which is  $k$ .

So, the correct answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 5:

Statement 1 is false because there are two vectors in  $\mathbb{R}^2$  that can be linearly dependent. For instance, if one vector is a scalar multiple of the other, then they are linearly dependent.

Statement 2 is true. By definition, if a set of vectors  $\{v_1, \dots, v_k\}$  spans  $V$  and are linearly independent, then they form a basis for  $V$ . The dimension of a vector space is defined as the number of vectors in any basis for the space, so in this case,  $\dim(V) = k$ .

So, the final answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 6:

Statement 1 is false. A set of two vectors in  $\mathbb{R}^2$  is linearly independent if and only if they are not scalar multiples of each other. If they are scalar multiples, they are linearly dependent.

Statement 2 is true. By definition, if  $V = \text{span}\{v_1, \dots, v_k\}$  and  $\{v_1, \dots, v_k\}$  are linearly independent, then the dimension of  $V$  is indeed  $k$ . The dimension of a vector space is the number of vectors in its basis, and a set of linearly independent vectors that spans the space is a basis.

So, the final answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 7:

Statement 1 is False. Two vectors are linearly dependent if one is a scalar multiple of the other. For example, the vectors  $(1,2)$  and  $(2,4)$  in  $\mathbb{R}^2$  are linearly dependent because  $(2,4)$  is twice  $(1,2)$ .

Statement 2 is True. If  $\{v_1, \dots, v_k\}$  are linearly independent, then none of these vectors can be written as a linear combination of the others. Hence, each vector adds a new dimension to the span, and the dimension of  $V$  is indeed  $k$ .

So, the final answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 8:

Statement 1 is false because if one vector is a scalar multiple of the other, then they are linearly dependent. For example, in  $\mathbb{R}^2$ , the vectors  $(1,2)$  and  $(2,4)$  are linearly dependent because  $(2,4)$  is 2 times  $(1,2)$ .

Statement 2 is true. The dimension of a vector space is the maximum number of linearly independent vectors in the space. If  $V$  is the span of  $\{v_1, \dots, v_k\}$  and these vectors are linearly independent, then they form a basis for  $V$ , and the dimension of  $V$  is indeed  $k$ .

Final Answer: D

\*\*\*\*\*

Answer Option 9:

Statement 1 is False. Not every set of two vectors in  $\mathbb{R}^2$  is linearly independent. For instance, the vectors  $[1, 2]$  and  $[2, 4]$  are not linearly independent because the second vector is a scalar multiple of the first.

Statement 2 is True. The dimension of a vector space is defined to be the maximum number of linearly independent vectors in the space. If a set  $\{v_1, \dots, v_k\}$  spans  $V$  and is linearly independent, by definition, the dimension of  $V$  must be  $k$ .

So, the final answer is D. 'False, True'

\*\*\*\*\*



Question 24:

'The set of all  $n$ th roots of unity under multiplication of complex numbers form a/an', A. 'semi group with identity', B. 'commutative semigroups with identity', C. 'group', D. 'abelian group'

=====

Answer Option 1:

The set of all  $n$ th roots of unity under multiplication of complex numbers form a/an 'abelian group'. Final answer: D

\*\*\*\*\*

Answer Option 2:

The set of all  $n$ th roots of unity under multiplication of complex numbers form an 'abelian group'. Final answer: D.

\*\*\*\*\*

Answer Option 3:

The  $n$ th roots of unity under multiplication of complex numbers form an 'abelian group'. This is because they satisfy all the conditions for a group - there is an identity (1), every element has an inverse (its conjugate), and the operation (multiplication) is associative and commutative. Therefore, the final answer is D.

\*\*\*\*\*

Answer Option 4:

The set of all  $n$ th roots of unity under multiplication of complex numbers form a/an 'abelian group'. This is because it is closed under multiplication, the multiplication operation is associative, every element has an inverse (the reciprocal of a root of unity is also a root of unity), and there is an identity element (1 is a root of unity). Additionally, the multiplication of complex numbers is commutative. Final Answer: D

\*\*\*\*\*

Answer Option 5:

The set of all  $n$ th roots of unity under multiplication of complex numbers form an 'abelian group'. This is because they satisfy all the group axioms, including closure, associativity, identity element (1 is the identity under multiplication), inverse elements (each  $n$ th root of unity has an inverse in the set), and commutativity (the order of multiplication doesn't matter). Hence, the answer is D. 'abelian group'.

\*\*\*\*\*

Answer Option 6:

The set of all  $n$ th roots of unity under multiplication of complex numbers form a/an 'abelian group'.

An abelian group is a set equipped with an associative operation (in this case, multiplication of complex numbers) that has an identity element (here, 1 is the identity as multiplying any complex number by 1 doesn't change its value) and every element has an inverse (each  $n$ th root of unity has an inverse which is also an  $n$ th root of unity). The operation is also commutative (the order of multiplication doesn't affect the result). So, the  $n$ th roots of unity form an abelian group. Final answer: D

\*\*\*\*\*

Answer Option 7:

The set of all  $n$ th roots of unity under multiplication of complex numbers form an 'abelian group'. This is because:

1. Closure: The product of any two  $n$ th roots of unity is also an  $n$ th root of unity.
2. Associativity: The product of complex numbers is associative.
3. Identity: The number 1 is an  $n$ th root of unity and serves as the identity element.
4. Inverse: Every  $n$ th root of unity has an inverse that is also an  $n$ th root of unity.
5. Commutativity: The product of complex numbers is commutative.

Hence, it is an 'abelian group'. Final Answer: D

\*\*\*\*\*

Answer Option 8:

The set of all  $n$ th roots of unity under multiplication of complex numbers forms an 'abelian group'. An abelian group is a group in which the binary operation is commutative, meaning the order of operations does not matter.

In this case, the binary operation is multiplication, the operation is commutative (since the order of multiplication doesn't change the result), the group has an identity element (1 is the multiplicative identity since any number multiplied by 1 gives the number itself), and each element has an inverse (the inverse of a number  $x$  in this group is its reciprocal  $1/x$ ).

So the correct answer is D. 'abelian group'.

\*\*\*\*\*

Answer Option 9:

The set of all  $n$ th roots of unity forms a group under multiplication of complex numbers.

The multiplication of complex numbers satisfies the four properties required for a set to be a group:

1. Closure: The product of any two  $n$ th roots of unity is another  $n$ th root of unity.
2. Associativity: The product of three  $n$ th roots of unity is the same no matter how they are grouped.
3. Identity: 1 is an  $n$ th root of unity and serves as the identity element because multiplying any  $n$ th root of unity by 1 does not change its value.
4. Inverse: Every  $n$ th root of unity has an inverse that is also an  $n$ th root of unity.

Moreover, the operation of multiplication of complex numbers is commutative, meaning that the order in which two  $n$ th roots of unity are multiplied does not affect the product. Thus, the set of all  $n$ th roots of unity forms an abelian group under multiplication of complex numbers. Final answer: D

\*\*\*\*\*



Question 25:

'Statement 1 | Every maximal ideal is a prime ideal. Statement 2 | If  $I$  is a maximal ideal of a commutative ring  $R$ , then  $R/I$  is field.', A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Both statements are true. In commutative ring theory, it is a well-known fact that every maximal ideal is indeed a prime ideal. Further, the quotient of a commutative ring by a maximal ideal results in a field.

This is one of the ways in which fields can be constructed in abstract algebra. So, the answer is A. 'True, True'.

\*\*\*\*\*

Answer Option 2:

Statement 1 is true: Every maximal ideal is indeed a prime ideal.

Statement 2 is also true: If  $I$  is a maximal ideal of a commutative ring  $R$ , then the quotient ring  $R/I$  is a field.

This is a fundamental result in ring theory, illustrating the close connection between the notions of maximal ideals, prime ideals, and fields.

So the final answer is A. 'True, True'

\*\*\*\*\*

Answer Option 3:

A. 'True, True'

The first statement is true. Every maximal ideal is a prime ideal. This is a known theorem in ring theory, a branch of abstract algebra.

The second statement is also true. If  $I$  is a maximal ideal of a commutative ring  $R$ , then  $R/I$  is a field. This is a fundamental property of maximal ideals and is used often in algebraic geometry and commutative algebra.

So, the correct answer is A. 'True, True'.

\*\*\*\*\*

Answer Option 4:

Statement 1: True. In a commutative ring with unity, every maximal ideal is indeed a prime ideal.

Statement 2: True. By definition, a maximal ideal is an ideal which is maximal in the set of all proper ideals of the ring. In other words, there are no other ideals contained between the maximal ideal and the entire ring. This property ensures that the factor ring ( $R/I$  in this case) is a field.

So, both statements are True. Final answer: A. 'True, True'.

\*\*\*\*\*

Answer Option 5:

Maximal ideals are always prime. This is because if  $I$  is a maximal ideal in a ring  $R$  and if  $I$  is not prime, then there exist  $a, b$  in  $R$  such that neither  $a$  nor  $b$  is in  $I$ , but  $ab$  is in  $I$ . However, this implies that the ideal generated by  $I$  and  $a$  strictly contains  $I$ , contradicting the maximality of  $I$ . So, statement 1 is true.

The quotient of a ring by a maximal ideal is indeed a field. This is a basic and well-known result in ring theory. The quotient ring  $R/I$  has no proper non-zero ideals, since any such ideal would correspond to an ideal of  $R$  properly containing  $I$ , contradicting the maximality of  $I$ . So, statement 2 is also true.

Therefore, the correct answer is A. 'True, True'.

\*\*\*\*\*

Answer Option 6:

Statement 1 | Every maximal ideal is a prime ideal.

This statement is true. By definition, a maximal ideal is an ideal that has no larger ideal containing it other than the ring itself. If a maximal ideal is not prime, we can find elements in the ring that can produce an ideal larger than the maximal ideal, which contradicts the definition of maximal ideal. Therefore, every maximal ideal must be a prime ideal.

Statement 2 | If  $I$  is a maximal ideal of a commutative ring  $R$ , then  $R/I$  is a field.

This statement is true. By the correspondence theorem, the ideals of  $R/I$  are in one-to-one correspondence with the ideals of  $R$  that contain  $I$ . Since  $I$  is maximal in  $R$ , the only ideal in  $R$  that contains  $I$  is  $R$  itself. This means that  $R/I$  has exactly two ideals, namely the zero ideal and  $R/I$  itself, which is the definition of a field.

Final Answer: A. 'True, True'

\*\*\*\*\*

Answer Option 7:

Statement 1: Every maximal ideal is a prime ideal. This statement is true. If  $I$  is a maximal ideal in a ring  $R$  and if  $ab$  is an element of  $I$ , where  $a$  and  $b$  are elements of  $R$ , then the ideal generated by  $I$  and  $a$  is either  $I$  or  $R$ . If it were  $R$  then  $a$  would be a unit and hence not in  $I$ . Thus, the ideal generated by  $I$  and  $a$  is  $I$  and so  $a$  is in  $I$ . This means that  $I$  is a prime ideal.

Statement 2: If  $I$  is a maximal ideal of a commutative ring  $R$ , then  $R/I$  is a field. This statement is also true. The quotient ring  $R/I$  has no ideals other than  $(0)$  and itself, which means it's a field.

So, both statements are true. Final answer: A. 'True, True'

\*\*\*\*\*

Answer Option 8:

Both statements are true.

Statement 1: Every maximal ideal is a prime ideal. This is a well-known result in ring theory. In a commutative ring, a maximal ideal is an ideal that is maximal in the set of all proper ideals, meaning it is not a proper subset of any other ideal. A prime ideal is an ideal with the property that the product of any two elements outside the ideal is not in the ideal. It can be shown that every maximal ideal is also a prime ideal.

Statement 2: If  $I$  is a maximal ideal of a commutative ring  $R$ , then  $R/I$  is a field. This is also a well-known result in ring theory. In a commutative ring, when you form the quotient ring  $R/I$  by a maximal ideal  $I$ , the result is a field. This is one of the characterizations of a maximal ideal.

So, the final answer is: A. 'True, True'

\*\*\*\*\*

Answer Option 9:

Statement 1: True. In ring theory, a branch of abstract algebra, a maximal ideal is an ideal that is maximal in the set of all proper ideals of the ring, i.e., it is an ideal  $I$  which is not equal to  $R$ , and such that if  $J$  is any ideal with  $I \subset J \subset R$ , then  $J = I$  or  $J = R$ .

Statement 2: True. If  $I$  is a maximal ideal of a commutative ring  $R$ , then  $R/I$  is a field. This is a fundamental theorem in ring theory which says that if  $A$  is a commutative ring, and  $I$  is an ideal contained in no other ideals except for the entire ring  $A$ , then the factor ring  $A/I$  is a field.

So, the correct answer is A. 'True, True'

\*\*\*\*\*

Question 26:

'Let  $G$  denote the set of all  $n \times n$  non-singular matrices with rational numbers as entries. Then under multiplication  $G$  is a/an', A. 'subgroup', B. 'finite abelian group', C. 'infinite, non abelian group', D. 'infinite, abelian'

=====

Answer Option 1:

The set of all  $n \times n$  non-singular matrices with rational numbers as entries form an infinite, non-abelian group under matrix multiplication. So, the answer is C. 'infinite, non abelian group'

\*\*\*\*\*

Answer Option 2:

The set of all  $n \times n$  non-singular matrices with rational numbers as entries, under multiplication, forms an infinite, non-abelian group. This is because the group operation (matrix multiplication) is not commutative. Final Answer: C

\*\*\*\*\*

Answer Option 3:

The set of all  $n \times n$  non-singular matrices with rational numbers as entries form an infinite, non-abelian group under multiplication. The group is infinite because there are infinite many such matrices. The group is non-abelian because matrix multiplication is not commutative. Hence, the answer is C.

\*\*\*\*\*

Answer Option 4:

The set of all  $n \times n$  non-singular matrices with rational numbers as entries under multiplication forms an infinite, non-abelian group. The group is infinite because there are infinitely many non-singular matrices. It is non-abelian because matrix multiplication is not commutative. Therefore, the correct answer is C. 'infinite, non abelian group'.

\*\*\*\*\*

Answer Option 5:

The set of all non-singular (i.e., invertible) matrices over the rational numbers, under the operation of multiplication, is an infinite, non-abelian group. This set is infinite because there are infinitely many such matrices, and it is non-abelian because matrix multiplication is generally not commutative. Hence, the correct answer is C. 'infinite, non abelian group'.

\*\*\*\*\*

Answer Option 6:

The set of all non-singular (invertible)  $n \times n$  matrices with rational numbers as entries is closed under multiplication, since the product of two invertible matrices is invertible. It also has an identity (the  $n \times n$  identity matrix), and every element has an inverse (its multiplicative inverse, which is also an invertible matrix). However, matrix multiplication is generally not commutative, so the group is non-abelian. It is also clearly infinite, since there are infinitely many rational numbers and thus infinitely many such matrices. So the group  $G$  is an infinite, non-abelian group. Final answer: C.

\*\*\*\*\*

Answer Option 7:

The correct answer is C. 'infinite, non abelian group'. A non-singular or invertible matrix is one that has an inverse, and the set of all such matrices forms a group under multiplication, because the product of two invertible matrices is also invertible, and the inverse of an invertible matrix is also invertible. This group is infinite because there are infinitely many rational numbers, and hence infinitely many such matrices. The group is not abelian because matrix multiplication is not commutative: for two matrices  $A$  and  $B$ , it is not generally the case that  $AB = BA$ .

\*\*\*\*\*

Answer Option 8:

The set of all  $n \times n$  non-singular matrices with rational numbers as entries is an infinite, non-abelian group under matrix multiplication, because:

- It is infinite because there are infinitely many rational numbers to choose from for each entry in the matrix.
- It is non-abelian because matrix multiplication is not commutative in general. In other words, for some matrices  $A$  and  $B$ , the product  $AB$  is not the same as the product  $BA$ .
- It is a group because it contains an identity element (the identity matrix), every element has an inverse (since the matrices are non-singular, they are invertible), and matrix multiplication is associative.

So the correct answer is C. 'infinite, non-abelian group'

\*\*\*\*\*

Answer Option 9:

A non-singular matrix is an invertible matrix, that is, a matrix which has a multiplicative inverse.

Under multiplication, the set of all non-singular matrices (of a given order  $n$ ) is a group because:

- (i) The product of two non-singular matrices is also non-singular.
- (ii) The product of matrices is associative.
- (iii) The identity matrix is non-singular.
- (iv) The inverse of a non-singular matrix is also non-singular.

However, matrix multiplication is not commutative in general, meaning that for any two matrices  $A$  and  $B$ ,  $AB \neq BA$ . So this group is not abelian.

Since the entries of the matrices are rational numbers, and there are infinitely many rational numbers, there are infinitely many such matrices.

Therefore,  $G$  is an infinite, non-abelian group. The final answer is: C.

\*\*\*\*\*

Question 27:

'Statement 1 | Every group of order 42 has a normal subgroup of order 7. Statement 2 | Every group of order 42 has a normal subgroup of order 8.'; A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1 is True. It follows from the Sylow theorems in group theory.

Statement 2 is False. There may not be any elements of order 8 in a group of order 42, let alone a normal subgroup of order 8.

Therefore the correct answer is C. 'True, False'.

\*\*\*\*\*

Answer Option 2:

Statement 1: True. By the Sylow theorems, a group of order  $42 = 6 \cdot 7$  has a normal subgroup of order 7.

Statement 2: False. A group of order 42 does not necessarily have a subgroup of order 8 as 8 is not a divisor of 42.

So, the correct answer is C. 'True, False'.

\*\*\*\*\*

Answer Option 3:

Statement 1 is true by Sylow's Theorem. Since 7 divides 42, there is a Sylow 7-subgroup. Also,  $7^2$  does not divide 42, and so the number of Sylow 7-subgroups is 1, so there is a normal subgroup of order 7.

Statement 2 is false. The order of a group is the number of its elements, and a subgroup of order 8 would imply that 8 divides 42, which is not the case.

So, the correct answer is C. 'True, False'

\*\*\*\*\*

Answer Option 4:

Statement 1: True. This is a consequence of the Sylow theorems. In particular, the third Sylow theorem implies that the number of 7-Sylow subgroups is congruent to 1 mod 7 and divides  $42/7 = 6$ . The only number satisfying these conditions is 1, so there is exactly one 7-Sylow subgroup, and this subgroup must be normal.

Statement 2: False. There is no guarantee of having a subgroup of order 8 in every group of order 42.

So, the correct answer is C. 'True, False'.

\*\*\*\*\*

Answer Option 5:

A group of order 42 factors as  $2 \cdot 3 \cdot 7$ . According to the Sylow theorems, the number of 7-Sylow subgroups (i.e., subgroups of order 7) divides 42 and is congruent to 1 mod 7. The only number that satisfies these is 1, so there is exactly one 7-Sylow subgroup and it is normal. Therefore, Statement 1 is true.

The number of 2-Sylow subgroups (i.e., subgroups of order  $2^2=4$ ) divides 42 and is congruent to 1 mod 2. There isn't a requirement that it be a multiple of 8, as 8 is not a factor of 42. Therefore, Statement 2 is false.

So, the correct answer is C. 'True, False'.

\*\*\*\*\*

Answer Option 6:

Statement 1 is true according to the Sylow theorems, which state that if a prime number  $p$  divides the order of a group and  $p^n$  is the highest power of  $p$  which does that, then there is a subgroup of order  $p^n$ , and any two such subgroups are conjugate. Furthermore, if the number of such subgroups, which is equal to the index of a Sylow  $p$ -subgroup, is equal to 1, then this subgroup is normal. The number  $42=2^1 \cdot 3^1 \cdot 7$ , and the only way to partition 42 into divisors 1 modulo 7 is 1 and 42, hence there is a normal subgroup of order 7.

Statement 2 is false. According to Sylow theorems, there cannot be a subgroup of order 8 in a group of order 42, because 8 does not divide 42.

So, the correct answer is C. 'True, False'.

\*\*\*\*\*

Answer Option 7:

Statement 1 is true because of Sylow's Theorem which states that if  $p$  is a prime that divides the order of a group  $G$ , then  $G$  has a subgroup of order  $p^n$  for every  $n$  such that  $p^n$  divides the order of  $G$ . In this case, 7 is a prime number that divides 42, and  $7^1 = 7$ , so, by Sylow's Theorem, every group of order 42 does have a subgroup of order 7.

Statement 2, however, is false. Again, by Sylow's Theorem, if  $p$  is a prime that divides the order of  $G$ , then  $G$  has a subgroup of order  $p^n$  for every  $n$  such that  $p^n$  divides the order of  $G$ .

In this case,  $8 = 2^3$ , but the highest power of 2 that divides 42 is  $2^1 = 2$ , not  $2^3 = 8$ . Therefore, by Sylow's Theorem, not every group of order 42 has a subgroup of order 8.

So, the final answer is C. 'True, False'

\*\*\*\*\*

Answer Option 8:

Statement 1 | Every group of order 42 has a normal subgroup of order 7. This is True. By the Sylow theorems, the number of Sylow 7-subgroups of a group of order 42 divides  $42/7=6$  and is congruent to 1 mod 7. The only number that satisfies these conditions is 1, so any group of order 42 has a unique (and therefore normal) Sylow 7-subgroup.

Statement 2 | Every group of order 42 has a normal subgroup of order 8. This is False. The order of a group is the number of its elements, and 8 does not divide 42, so a group of order 42 cannot have a subgroup of order 8.

So the correct answer is C. 'True, False'.

\*\*\*\*\*

Answer Option 9:

The Sylow first theorem tells us that any group of order  $p^n m$  with  $p$  prime and  $p \nmid m$  has at least one Sylow  $p$ -subgroup of order  $p^n$ . The Sylow second theorem then tells us that all Sylow  $p$ -subgroups are conjugate, and are therefore isomorphic. In particular, if there is only one Sylow  $p$ -subgroup, it must be invariant under conjugation and is therefore normal.

The order of a group is the number of its elements. Here the orders are 42 and 8. The prime factorization of 42 is  $2 \cdot 3 \cdot 7$ , so by the Sylow theorems, every group of order 42 has a Sylow 7-subgroup, and if there is only one such subgroup, it is normal. So statement 1 is true.

However, 8 is  $2^3$ , and 42 is not divisible by  $2^4$ , so again by the Sylow theorems, a group of order 42 cannot have a subgroup of order 8, let alone a normal one. Statement 2 is false.

So the correct answer is C. 'True, False'.

\*\*\*\*\*

Question 28:

'Determine whether the polynomial in  $\mathbb{Z}[x]$  satisfies an Eisenstein criterion for irreducibility over  $\mathbb{Q}$ .  $8x^3 + 6x^2 - 9x + 24$ ', A. 'Yes, with  $p=2$ .', B. 'Yes, with  $p=3$ .', C. 'Yes, with  $p=5$ .', D. 'No.'

=====

Answer Option 1:

The Eisenstein criterion requires a prime number  $p$  such that  $p$  divides each of the coefficients of the polynomial apart from the leading coefficient, and  $p^2$  does not divide the constant term. For the polynomial  $8x^3 + 6x^2 - 9x + 24$ , 2 and 3 both divide 6 and 9, but neither  $2^2=4$  nor  $3^2=9$  divides 24. Therefore, the polynomial does not satisfy an Eisenstein criterion for irreducibility over  $\mathbb{Q}$ . Final answer:

D

=====

Answer Option 2:

The Eisenstein criterion states that a polynomial is irreducible if there is a prime number  $p$  such that  $p$  divides each coefficient of the polynomial except the leading coefficient,  $p$  does not divide the leading coefficient, and  $p^2$  does not divide the constant term. In the given polynomial,  $8x^3 + 6x^2 - 9x + 24$ , there is no such prime number that satisfies all these conditions. Therefore, the answer is D. 'No.'

=====

Answer Option 3:

The Eisenstein criterion requires a prime  $p$  such that  $p$  divides each coefficient of  $x^{n-1}, x^{n-2}, \dots, x^1, x^0$ ,  $p$  does not divide the leading coefficient, and  $p^2$  does not divide the constant term.

For the polynomial  $8x^3 + 6x^2 - 9x + 24$ , the only prime that divides 6, -9, and 24 (ignoring sign) but not 8 is 3. However,  $3^2 = 9$ , which does not divide 24.

So, the answer is D, the polynomial does not satisfy an Eisenstein criterion.

=====

Answer Option 4:

The Eisenstein criterion states that if there is a prime number  $p$  such that  $p$  divides all the coefficients of a polynomial except the leading coefficient,  $p^2$  does not divide the constant term, and  $p$  does not divide the leading coefficient, then the polynomial is irreducible over  $\mathbb{Q}$ .

Looking at the given polynomial, we can see that 3 divides all the coefficients except the leading coefficient,  $3^2$  does not divide the constant term but 2 does not divide the leading coefficient. Therefore, the polynomial satisfies an Eisenstein criterion for irreducibility over  $\mathbb{Q}$  with  $p=3$ .

Final answer: B. 'Yes, with  $p=3$ .'

=====

Answer Option 5:

The Eisenstein criterion for irreducibility is that if there is a prime number  $p$  such that  $p$  divides each of the coefficients in the polynomial except for the leading coefficient,  $p$  squared does not divide the constant term, and  $p$  does not divide the leading coefficient, then the polynomial is irreducible over  $\mathbb{Q}$ .

Looking at the polynomial  $8x^3 + 6x^2 - 9x + 24$ , we can see that 3 divides 6, -9, and 24 but not 8, but 3 squared does not divide 24. So the Eisenstein criterion for irreducibility is satisfied with  $p=3$ . So the correct answer is: B. 'Yes, with  $p=3$ .'

=====

Answer Option 6:

For the Eisenstein criterion to hold, we need a prime  $p$  such that  $p$  divides all coefficients but the leading one,  $p^2$  does not divide the constant term, and  $p$  does not divide the leading coefficient. In this case, we see that 3 divides 6, -9 and 24 but not 8, and  $3^2$  does not divide 24, so the polynomial satisfies the Eisenstein criterion at  $p=3$ . So, the answer is B. 'Yes, with  $p=3$ .'

=====

Answer Option 7:

The Eisenstein's criterion states that a polynomial is irreducible over  $\mathbb{Q}$  if there exists a prime number  $p$  such that:

1.  $p$  divides each constant term  $a_i$  for  $i < n$ , but  $p^2$  does not divide  $a_0$ .
2.  $p$  does not divide  $a_n$  (the leading coefficient).

In this polynomial, the coefficients are 8, 6, -9, and 24. The number that divides all the coefficients except the leading coefficient (8) is 3, but  $3^2=9$  does not divide the constant term 24. Therefore, the polynomial is irreducible by Eisenstein's Criterion with  $p=3$ . Final Answer: B. 'Yes, with  $p=3$ .'

=====

Answer Option 8:

The Eisenstein criterion for irreducibility over  $\mathbb{Q}$  states that if there is a prime number  $p$  such that:

- i)  $p$  divides all coefficients of the polynomial except the leading coefficient,
- ii)  $p^2$  does not divide the constant term, and
- iii)  $p$  does not divide the leading coefficient,

then the polynomial is irreducible over  $\mathbb{Q}$ .

Here, we have the polynomial  $8x^3 + 6x^2 - 9x + 24$ . The prime number 3 divides all coefficients except the leading coefficient, and  $3^2$  does not divide the constant term 24. However, 3 does divide the leading coefficient 8, so the Eisenstein criterion is not satisfied for any prime  $p$ .

So, the answer is D. 'No.'

=====

Answer Option 9:

The Eisenstein criterion states that a polynomial  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  in  $\mathbb{Z}[x]$  is irreducible over  $\mathbb{Q}$  if there is a prime number  $p$  such that:



-  $p$  divides  $a_i$  for  $i = 0, 1, \dots, n-1$ ;

-  $p$  does not divide  $a_n$ ; and

-  $p^2$  does not divide  $a_0$ .

In this case, the polynomial is  $f(x) = 8x^3 + 6x^2 - 9x + 24$ .

We can see that the prime number  $p=3$  divides the coefficients of  $x^2$ ,  $x$ , and the constant term, but it does not divide the coefficient of  $x^3$ . Also,  $3^2$  does not divide the constant term.

Therefore, the polynomial satisfies the Eisenstein criterion with  $p=3$ , so the correct answer is B. 'Yes, with  $p=3$ '.

\*\*\*\*\*

Question 29:

'Statement 1 | The image of a group of 6 elements under a homomorphism may have 12 elements. Statement 2 | There is a homomorphism of some group of 6 elements into some group of 12 elements.', A.

'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1 is False. A homomorphism cannot increase the number of elements in a set.

Statement 2 is True. There can indeed be a homomorphism from a group of 6 elements to a group of 12 elements (for example, the homomorphism could send every element in the first group to the identity in the second group).

So, the correct answer is D: 'False, True'.

=====

Answer Option 2:

Statement 1: False. By the definition of a homomorphism, the image of a group cannot have more elements than the group itself, because each element of the group maps to exactly one element in the image.

Statement 2: True. While the image of the group cannot have more elements than the group itself, it is certainly possible for a group of 6 elements to be mapped into a larger group (for example, all elements may be mapped to a single element in the larger group).

So, the answer is D. 'False, True'.

=====

Answer Option 3:

Statement 1 is false. A group homomorphism maps the identity to the identity, and by definition preserves group operations, so cannot send distinct elements to distinct elements. Therefore, the image of a group under a homomorphism cannot have more elements than the originating group.

Statement 2 is true. The trivial homomorphism, which maps all elements of the originating group to the identity of the target group, is a valid homomorphism from a group of 6 elements to a group of 12 elements.

Final answer: D. 'False, True'

=====

Answer Option 4:

A homomorphism preserves the operation structure of a group. Therefore, the image of any group under a homomorphism can't have more elements than the original group. So, Statement 1 is False.

However, there can be a homomorphism from a group of 6 elements to a group of 12 elements. This is because a homomorphism can map multiple elements from the original group to the same element in the target group (making the image smaller than the target group). So, Statement 2 is True.

Final answer: D. 'False, True'.

=====

Answer Option 5:

Homomorphisms preserve the group structure. Specifically, one key property is that the number of elements in the image of the homomorphism cannot exceed the number of elements in the original group. Therefore, statement 1 is false because the image cannot have more elements than the original group does.

However, statement 2 is true. There could be a homomorphism from a group with 6 elements to a group with 12 (or more) elements. For instance, the homomorphism could send all elements of the original group to a single identity element in the larger group (this is known as the trivial homomorphism). So, the correct choice is D 'False, True'.

=====

Answer Option 6:

Statement 1 | The image of a group of 6 elements under a homomorphism may have 12 elements. This is false. The image of a group under a homomorphism must be a subgroup of the codomain group.

Since the size of a subgroup must divide the size of the group, a group of 6 elements can't map to 12 elements under a homomorphism.

Statement 2 | There is a homomorphism of some group of 6 elements into some group of 12 elements. This is true. For example, consider the trivial homomorphism from any group of 6 elements to any group of 12 elements that maps all elements in the domain to the identity element in the codomain.

So the answer is False, True. Final answer: D.

=====

Answer Option 7:

Statement 1 is false because a homomorphism preserves the structure of a group. If the original group has 6 elements, the image cannot have more than 6 elements.

Statement 2 is true because a homomorphism can map a group into a larger group. For example, consider the group of integers modulo 6 under addition, and the group of integers modulo 12 under addition.

The map that sends an integer  $n$  modulo 6 to  $2n$  modulo 12 is a homomorphism from the first group to the second.

Thus, the correct answer is D. 'False, True'.

=====

Answer Option 8:

Statement 1 is false. By definition, a homomorphism maps a group to a group in a way that preserves the group structure. If the original group has 6 elements, the image under the homomorphism cannot have more than 6 elements since the homomorphism maps each element in the original group to an element in the image.

Statement 2 is true. For example, consider the homomorphism that maps the cyclic group of 6 elements,  $Z_6$ , to the group  $Z_{12}$  under addition. We can define the homomorphism  $f: Z_6 \rightarrow Z_{12}$  (where  $f$  is a function from  $Z_6$  to  $Z_{12}$ ) as  $f(x) = 2x$  for all  $x$  in  $Z_6$ . This is a valid homomorphism. The image under this homomorphism is the subset  $\{0, 2, 4, 6, 8, 10\}$  of  $Z_{12}$  which has exactly 6 elements.

So, the answer is D. 'False, True'.

Final Answer: D

\*\*\*\*\*

Answer Option 9:

Statement 1 | The definition of a homomorphism restricts that the image of a group of 6 elements cannot have more elements than the pre-image. Therefore, the image of a group of 6 elements under a homomorphism can't have 12 elements. Statement 1 is False.

Statement 2 | While a homomorphism maps a group into another group, the image of the homomorphism (the elements in the target group that actually get mapped to) need not be the entire target group. In particular, it can be a smaller subgroup of the target group. Therefore, there can indeed exist a homomorphism from a group of 6 elements into a group of 12 elements, for example mapping the group of 6 elements into a subgroup of the group with 12 elements. Statement 2 is True.

Final answer: D

\*\*\*\*\*

Question 30:

'Statement 1 | The homomorphic image of a cyclic group is cyclic. Statement 2 | The homomorphic image of an Abelian group is Abelian.', A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Both statements are true. The homomorphic image of a cyclic group is cyclic because a homomorphism preserves the group operation, and therefore preserves the cyclic property of the group. The homomorphic image of an Abelian group is Abelian because a homomorphism preserves the group operation, and therefore preserves the commutative property of the group. Final Answer: A. 'True, True'

\*\*\*\*\*

Answer Option 2:

Statement 1 is True. If a group is cyclic, i.e., generated by a single element, then its homomorphic image is also generated by the image of that single element, hence is cyclic.

Statement 2 is True. If a group is Abelian, i.e., its operation is commutative, then its homomorphic image is also commutative, hence is Abelian.

So the final answer is A. 'True, True'.

\*\*\*\*\*

Answer Option 3:

Both statements are true.

Statement 1: The homomorphic image of a cyclic group is cyclic. This is true because a cyclic group is generated by a single element, and the image of the generating element will generate the image of the group.

Statement 2: The homomorphic image of an Abelian group is Abelian. This is true because if  $x$  and  $y$  are elements of an Abelian group, then  $x \cdot y = y \cdot x$ , and the image of the product is the product of the images, which preserves the Abelian property.

Final answer: A. 'True, True'

\*\*\*\*\*

Answer Option 4:

Both statements are true.

Statement 1: The image of a group homomorphism applied to a cyclic group results in a cyclic group. This is because a cyclic group is generated by a single element, and the homomorphic image of that generator will generate the image group.

Statement 2: The image of a group homomorphism applied to an Abelian (commutative) group results in an Abelian group. This is because the homomorphism preserves the group operation, so if the original group was commutative, so too will be the image group.

Final Answer: A. 'True, True'

\*\*\*\*\*

Answer Option 5:

Both statements are True.

Statement 1: The homomorphic image of a cyclic group is cyclic. This is true because a homomorphism preserves the operation structure of a group. Since a cyclic group is generated by a single element, its image under a homomorphism will also be generated by the image of that single element, making it cyclic.

Statement 2: The homomorphic image of an Abelian group is Abelian. This is true because a homomorphism preserves the commutative property of a group. If the original group is Abelian (commutative), so will be its image under a homomorphism.

Final Answer: A

\*\*\*\*\*

Answer Option 6:

The homomorphic image of a cyclic group is cyclic. This is true, as any homomorphism sends generators to generators, and therefore cyclic groups to cyclic groups.

The homomorphic image of an Abelian group is Abelian. This is also true. If  $G$  is an Abelian group and  $\phi: G \rightarrow H$  is a homomorphism, then for any  $a, b \in G$ , we have  $\phi(ab) = \phi(a)\phi(b) = \phi(b)\phi(a) = \phi(ba)$ , showing that  $H$  is Abelian.

Final Answer: A. 'True, True'

\*\*\*\*\*

Answer Option 7:

Statement 1 is true. If the group  $G$  is cyclic, then there is some element  $a$  such that every element of  $G$  can be written as a power of  $a$ . The homomorphic image of  $G$  under a homomorphism  $f$  is a group whose elements are  $f(a^k)$  for various integers  $k$ , and this is certainly a cyclic group.

Statement 2 is also true. An Abelian group is one in which the operation is commutative, so for any elements  $a$  and  $b$  of the group,  $ab=ba$ . A homomorphism  $f$  preserves this property, so if  $G$  is Abelian, so is its homomorphic image.

So the final answer is A. 'True, True'

\*\*\*\*\*

Answer Option 8:

A homomorphism preserves the group operation, so if we have a cyclic group that's generated by a single element, its image will also be generated by the image of that element, making it cyclic. So,

Statement 1 is true.

Regarding Statement 2, consider two elements  $a$  and  $b$  in an Abelian group  $G$ . Because  $G$  is abelian,  $a*b = b*a$ . A group homomorphism  $f$  preserves this property. That is,  $f(a)*f(b) = f(b)*f(a)$  for all  $a, b$  in  $G$ . Therefore, the homomorphic image of an abelian group is also abelian. So, Statement 2 is true.

Final Answer: A. 'True, True'

\*\*\*\*\*

Answer Option 9:

Both statements are true.

Statement 1: The homomorphic image of a cyclic group is cyclic. This is because if  $G$  is a cyclic group and  $\phi$  is a homomorphism from  $G$  to  $H$ , then the image of  $G$  under  $\phi$ , which is the set  $\phi[G] = \{\phi(g) \mid g \in G\}$ , is a cyclic subgroup of  $H$ .

Statement 2: The homomorphic image of an Abelian group is Abelian. This is because if  $G$  is an Abelian group and  $\phi$  is a homomorphism from  $G$  to  $H$ , then for any  $g_1, g_2 \in G$ , we have  $\phi(g_1 g_2) = \phi(g_1) \phi(g_2) = \phi(g_2) \phi(g_1)$ , where the second equality follows because  $G$  is Abelian. This shows that  $\phi[G]$  is an Abelian subgroup of  $H$ .

Final answer: A. 'True, True'.

\*\*\*\*\*

Question 31:

'Statement 1 | If  $H$  is a subgroup of a group  $G$  and  $a$  belongs to  $G$ , then  $aH = Ha$ . Statement 2 | If  $H$  is normal of  $G$  and  $a$  belongs to  $G$ , then  $ah = ha$  for all  $h$  in  $H$ .' A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1 is false. The equality  $aH = Ha$  holds for all  $a$  in  $G$  if and only if  $H$  is a normal subgroup of  $G$ .

Statement 2 is true. By definition, a subgroup  $H$  of  $G$  is normal if and only if  $ah = ha$  for all  $a$  in  $G$  and  $h$  in  $H$ .

Final Answer: D. 'False, True'

\*\*\*\*\*

Answer Option 2:

Statement 1 is false. The condition given in Statement 1 is not always true for all subgroups, it is only valid for normal subgroups. In general, for a subgroup  $H$  of a group  $G$ ,  $aH$  can be different from  $Ha$ .

Statement 2 is true. By definition, a subgroup  $H$  of a group  $G$  is normal if and only if  $ah = ha$  for all  $a$  in  $G$  and  $h$  in  $H$ .

Final answer: D. 'False, True'

\*\*\*\*\*

Answer Option 3:

Statement 1 is false. If  $H$  is just a subgroup of  $G$ , it doesn't necessarily mean that left and right cosets are equal, i.e.,  $aH = Ha$  may not hold true in every case.

Statement 2 is true. By definition, if  $H$  is a normal subgroup of  $G$ , then for any  $a$  in  $G$  and  $h$  in  $H$ , the condition  $ah = ha$  always holds for all  $h$  in  $H$ .

So, the solution is D. 'False, True'.

\*\*\*\*\*

Answer Option 4:

Statement 1 is false. Not all subgroups have the property that  $aH = Ha$  for all  $a$  in  $G$ . This property is specific to normal subgroups.

Statement 2 is true. This is the definition of a normal subgroup: if  $H$  is a normal subgroup of  $G$  and  $a$  is in  $G$ , then  $ah = ha$  for all  $h$  in  $H$ .

So, the final answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 5:

Statement 1 is false. If  $H$  is a subgroup of a group  $G$  and  $a$  belongs to  $G$ , then  $aH = Ha$  is not always true. This is true only for the case when  $H$  is a normal subgroup of  $G$ .

Statement 2 is true. By definition, a subgroup  $H$  of a group  $G$  is normal if and only if  $ah = ha$  for all  $a$  in  $G$  and  $h$  in  $H$ .

Final answer: D. 'False, True'

\*\*\*\*\*

Answer Option 6:

Statement 1 is false, and statement 2 is true. For a subgroup  $H$  of  $G$ ,  $aH = Ha$  for every  $a$  in  $G$  if and only if  $H$  is a normal subgroup of  $G$ . So, simply having  $H$  as a subgroup of  $G$  does not guarantee  $aH = Ha$ .

For statement 2,  $ah = ha$  for every  $h$  in  $H$  is the definition of a normal subgroup. So, if  $H$  is normal of  $G$ , then by definition,  $ah = ha$  for all  $h$  in  $H$ . Final Answer: D

\*\*\*\*\*

Answer Option 7:

Statement 1 is false. If  $H$  is a subgroup of a group  $G$  and  $a$  belongs to  $G$ , then  $aH = Ha$  only if  $H$  is a normal subgroup of  $G$ .

Statement 2 is true. By definition, a subgroup  $H$  of a group  $G$  is normal if and only if  $ah = ha$  for all  $a$  in  $G$  and  $h$  in  $H$ .

So the correct answer would be D. 'False, True'

\*\*\*\*\*

Answer Option 8:

Statement 1 is false. In general, for a subgroup  $H$  of  $G$  and an element  $a$  in  $G$ , it's not necessarily true that left coset  $aH$  is equal to the right coset  $Ha$ . This is only guaranteed if  $H$  is a normal subgroup of  $G$ .

Statement 2 is true. If  $H$  is a normal subgroup of  $G$  and  $a$  is an element of  $G$ , then for every  $h$  in  $H$ ,  $ah = ha$ . This is one of the properties that defines a normal subgroup.

So the answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 9:

Statement 1 is false. If  $H$  is simply a subgroup of  $G$  and  $a$  belongs to  $G$ , we don't have the guarantee that  $aH$  (the left coset) equals  $Ha$  (the right coset). This is true only if  $H$  is a normal subgroup of  $G$ .

Statement 2 is true. The definition of a normal subgroup is that, for every  $a$  in  $G$  and every  $h$  in  $H$ , we have  $ah = ha$ . This is also known as the "commutativity" property within the group.

So, the correct answer is D. 'False, True'.

\*\*\*\*\*

Question 32:

'If  $(G, \cdot)$  is a group such that  $(ab)^{-1} = a^{-1}b^{-1}$ , for all  $a, b$  in  $G$ , then  $G$  is a/an', A. 'commutative semi group', B. 'abelian group', C. 'non-abelian group', D. 'None of these'

=====

Answer Option 1:

B. 'abelian group'

=====

Answer Option 2:

B. 'abelian group'

=====

Answer Option 3:

B. 'abelian group'

=====

Answer Option 4:

The property  $(ab)^{-1} = a^{-1}b^{-1}$  for all  $a, b$  in  $G$  is known as the "abelian property" and is characteristic of abelian groups. Therefore,  $G$  is an abelian group. Final Answer: B.

=====

Answer Option 5:

To have  $(ab)^{-1} = a^{-1}b^{-1}$ , the group  $G$  must be abelian, which means the group operation is commutative. Therefore, the correct answer is B. 'abelian group'.

=====

Answer Option 6:

In the given condition,  $(ab)^{-1} = a^{-1}b^{-1}$ , we see that the reverse of the product of  $a$  and  $b$  is equal to the product of their inverses in reverse order. This suggests that the operation in the group is commutative. In other words,  $ab = ba$  for all  $a$  and  $b$  in  $G$ . Therefore, the group is Abelian. So, the correct answer is B. 'abelian group'.

=====

Answer Option 7:

The property that  $(ab)^{-1} = a^{-1}b^{-1}$  holds for all  $a, b$  in a group  $G$  is not exclusive to any specific type of group—it is a general property of groups. However, if we apply this property twice, we get  $(a^{-1}b^{-1})^{-1} = (b^{-1})^{-1}(a^{-1})^{-1} = ba$ , which is equivalent to  $ab = ba$ . So every element in the group commutes with every other element, which means  $G$  is an abelian group. So the answer is B. 'abelian group'.

=====

Answer Option 8:

In group theory, a group is said to be abelian or commutative if the group operation is commutative, i.e., if for all  $a$  and  $b$  in  $G$ ,  $ab = ba$ . From the given condition,  $(ab)^{-1} = a^{-1}b^{-1}$ . By the definition of a group, we have  $(ab)^{-1} = b^{-1}a^{-1}$  (since the inverse of a product is the product of the inverses in reverse order). Comparing the two equalities, we can see that  $a^{-1}b^{-1} = b^{-1}a^{-1}$ . This implies that  $ab = ba$  for all  $a, b$  in  $G$ . Hence,  $G$  is a commutative or abelian group. So, the correct answer is B. 'abelian group'.

=====

Answer Option 9:

The given condition can be rewritten as  $(ab)^{-1} = b^{-1}a^{-1}$ , which is the definition of the inverse of the product in a group, without any further constraints. However, if we multiply both sides of the equation by  $ab$  (which is allowed because every element in a group has an inverse), we get  $e = b^{-1}a^{-1}ab$ , where  $e$  is the group's identity. This simplifies to  $b^{-1}a^{-1}ab = e$ . Now, multiplying both sides by  $a^{-1}b$  on the right gives us  $b^{-1} = b^{-1}$ , which holds for all  $b$  in  $G$ , so the group must be an abelian group where the operation is commutative. Final Answer: B.

=====

Question 33:

'Statement 1 | In a finite dimensional vector space every linearly independent set of vectors is contained in a basis. Statement 2 | If  $B_1$  and  $B_2$  are bases for the same vector space, then  $|B_1| = |B_2|$ .' A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

In a finite dimensional vector space, every linearly independent set of vectors can be expanded, if necessary, to form a basis (Statement 1: True). Secondly, the number of elements in any basis for a vector space is always the same and is known as the dimension of the vector space (Statement 2: True). Therefore, the final answer is  $\boxed{\text{A. 'True, True'}}$ .

\*\*\*\*\*

Answer Option 2:

Statement 1: True. In a finite dimensional vector space, a linearly independent set of vectors can always be extended to form a basis.

Statement 2: True. Any two bases of the same vector space have the same cardinality. This is known as the dimension theorem.

So, both statements are true. Final Answer: A. 'True, True'

\*\*\*\*\*

Answer Option 3:

Statement 1 is true. This is a standard result in linear algebra: any linearly independent set in a finite-dimensional vector space can be extended to a basis.

Statement 2 is also true. The number of elements in a basis for a vector space is called the dimension of the space. All bases for a given vector space must have the same number of elements, so  $|B_1| = |B_2|$ .

Therefore, the correct answer is A. 'True, True'

\*\*\*\*\*

Answer Option 4:

Statement 1: True. In a finite dimensional vector space, every linearly independent set of vectors can be extended to form a basis.

Statement 2: True. The number of vectors in a basis for a vector space is constant, and this number is known as the dimension of the vector space. Therefore, if  $B_1$  and  $B_2$  are bases for the same vector space, they must have the same number of vectors.

Final Answer: A. 'True, True'

\*\*\*\*\*

Answer Option 5:

Both Statement 1 and Statement 2 are true.

Statement 1 | It is a known property of vector spaces that every linearly independent set of vectors can be extended to form a basis for the space.

Statement 2 | By definition, a basis for a vector space is a set of vectors that spans the space and is linearly independent. Hence, any two bases for the same vector space must have the same number of elements.

So, the correct answer is A. 'True, True'.

\*\*\*\*\*

Answer Option 6:

Statement 1 | True: In a finite-dimensional vector space, any set of linearly independent vectors can be extended to a basis by adding other vectors from the vector space, if necessary.

Statement 2 | True: All bases for a vector space have the same number of elements (this number is known as the dimension of the vector space). Thus, if  $B_1$  and  $B_2$  are bases for the same vector space, then  $|B_1| = |B_2|$ .

So the correct answer is A. 'True, True'.

\*\*\*\*\*

Answer Option 7:

Statement 1 is true. In a finite dimensional vector space, every linearly independent set of vectors can be extended to a basis. This is a fundamental result in linear algebra.

Statement 2 is also true. All bases of a single vector space must have the same cardinality. This cardinality is known as the dimension of the space.

So, both statements are True. Final answer: A

\*\*\*\*\*

Answer Option 8:

Both Statement 1 and Statement 2 are true.

Statement 1: In a finite dimensional vector space, any linearly independent set of vectors can be extended to a basis. This is because if the set is not yet a basis (i.e., it doesn't span the entire space), there must exist a vector in the space not in the span of the set. This vector can be added to the set to form a larger linearly independent set. This process can be repeated until we have a basis.

Statement 2: The bases of a vector space always have the same cardinality. This is a fundamental property of bases - any two bases for a vector space must have the same number of elements. This common number of elements is called the dimension of the vector space.

So, the correct answer is A. 'True, True'.

\*\*\*\*\*

Answer Option 9:



Statement 1: True. If a set of vectors is linearly independent, we can keep adding vectors (which are not linear combinations of the existing vectors) to the set until we cannot add more without losing the linear independence. The resulting set will be a basis that contains our original set.

Statement 2: True. A basis is a set of vectors that spans the vector space and is linearly independent. The size of the basis (number of vectors in the basis) is equal to the dimension of the vector space, and the dimension of a vector space is unique. Therefore, any two bases for the same vector space must contain the same number of vectors.

So, the correct answer is A. 'True, True'.

\*\*\*\*\*

Question 34:

'Some group  $(G, 0)$  is known to be abelian. Then which one of the following is TRUE for  $G$ ?', A. ' $g = g^{-1}$  for every  $g$  in  $G$ ', B. ' $g = g^2$  for every  $g$  in  $G$ ', C. ' $(g \circ h)^2 = g^2 \circ h^2$  for every  $g, h$  in  $G$ ', D. ' $G$  is of finite order'

=====

Answer Option 1:

An abelian group is defined as a group in which the group operation is commutative. This means that the operation of any two elements in the group is independent of their order. So, the statement ' $(g \circ h)^2 = g^2 \circ h^2$  for every  $g, h$  in  $G$ ' is true for abelian group. Final answer: C

\*\*\*\*\*

Answer Option 2:

An Abelian group is a group in which the binary operation is commutative, that is, for all  $g, h$  in  $G$ ,  $g \circ h = h \circ g$ . The property that holds for all  $g, h$  in  $G$  in an Abelian group is  $(g \circ h)^2 = g^2 \circ h^2$ . So, the final answer is C.

\*\*\*\*\*

Answer Option 3:

In an abelian group, the order of operations does not matter, meaning  $gh=hg$  for any elements  $g$  and  $h$  in  $G$ . From this we can derive the third option by taking the square on both sides  $(gh)^2 = (hg)^2$  which leads to  $g^2h^2=h^2g^2$ . Therefore, the correct answer is (C) ' $(g \circ h)^2 = g^2 \circ h^2$  for every  $g, h$  in  $G$ '. The other options are not necessarily true for all abelian groups. Final Answer: C.

\*\*\*\*\*

Answer Option 4:

In an abelian group, the operation is commutative. Therefore, for all  $g, h$  in  $G$ , we have  $(g \circ h) = (h \circ g)$ . Replacing  $g$  and  $h$  with  $(g \circ h)$  and  $(g \circ h)$  respectively, we get  $(g \circ h)^2 = (h \circ g)^2$ , which is the same as  $g^2 \circ h^2$ . Therefore, the statement C. ' $(g \circ h)^2 = g^2 \circ h^2$  for every  $g, h$  in  $G$ ' is TRUE for an abelian group. Final Answer: C

\*\*\*\*\*

Answer Option 5:

An abelian group is a group in which the binary operation is commutative, i.e., for every  $g, h$  in  $G$ ,  $g \circ h = h \circ g$ .

This property does not guarantee that ' $g = g^{-1}$  for every  $g$  in  $G$ ' or ' $g = g^2$  for every  $g$  in  $G$ ' or ' $G$  is of finite order'. However, it does guarantee that ' $(g \circ h)^2 = g^2 \circ h^2$  for every  $g, h$  in  $G$ ', as we can see by expanding each side:

$$(g \circ h)^2 = (g \circ h) \circ (g \circ h) = g \circ (h \circ g) \circ h = g^2 \circ h^2$$

Therefore, the correct answer is C. So, the final answer: C

\*\*\*\*\*

Answer Option 6:

The property of being abelian (or commutative) means that the order in which elements are combined does not matter. That is, for any elements  $g$  and  $h$  in  $G$ ,  $g \circ h = h \circ g$ . Looking at the options, only option C: ' $(g \circ h)^2 = g^2 \circ h^2$  for every  $g, h$  in  $G$ ' is guaranteed to be true in an abelian group. This is a restatement of the abelian property:

$$(g \circ h)^2 = (g \circ h) \circ (g \circ h) = g \circ (h \circ g) \circ h = g \circ g \circ h \circ h = g^2 \circ h^2.$$

So, the correct answer is C.

\*\*\*\*\*

Answer Option 7:

For an abelian group  $(G, 0)$ , the property that holds is C: ' $(g \circ h)^2 = g^2 \circ h^2$  for every  $g, h$  in  $G$ '.

In an abelian group, the group operation is commutative, which means that for every  $g, h$  in  $G$ ,  $g \circ h = h \circ g$ . Therefore,  $(g \circ h)^2 = g^2 \circ h^2$ .

The other options do not necessarily hold for all abelian groups. For example, it is not necessary that every element is its own inverse (option A) or that every element is its own square (option B). Also, abelian groups can be of infinite order (option D).

Final Answer: C

\*\*\*\*\*

Answer Option 8:

An abelian group is a group in which the binary operation is commutative, that is for all  $g, h$  in  $G$ ,  $g \circ h = h \circ g$ . Option C states that  $(g \circ h)^2 = g^2 \circ h^2$  for every  $g, h$  in  $G$ , which is true for all abelian groups. So the correct answer is C.

Options A and B are not necessarily true for all abelian groups. For example, consider the additive group of integers. It is abelian but 2 is not equal to -2 (option A) and 2 is not equal to 4 (option B).

Option D is also not necessarily true for all abelian groups. For example, the additive group of integers is abelian and infinite.

Final Answer: C

\*\*\*\*\*

Answer Option 9:

An abelian group is a group in which the binary operation is commutative, i.e., for all  $g$  and  $h$  in  $G$ ,  $g \circ h = h \circ g$ . However, this does not imply that  $g = g^{-1}$  for every  $g$  in  $G$  (A is false). This also does not imply that  $g = g^2$  for every  $g$  in  $G$  (B is false). An abelian group can be infinite, so D is also false.

However, for every  $g, h$  in  $G$ , we have  $(g \circ h)^2 = g \circ h \circ g \circ h = g \circ g \circ h \circ h = g^2 \circ h^2$  because of the commutativity of the operation. Therefore, option C is TRUE for an abelian group. Final Answer: C

\*\*\*\*\*

Question 35:

'Statement 1 | If  $T: V \rightarrow W$  is a linear transformation and  $\dim(V) < \dim(W) < 1$ , then  $T$  must be injective. Statement 2 | Let  $\dim(V) = n$  and suppose that  $T: V \rightarrow V$  is linear. If  $T$  is injective, then it is a bijection.'

A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1 is false. If the dimension of the domain of a linear transformation is less than the dimension of the codomain, the transformation can be either injective or not injective. So the statement is not necessarily true. Statement 2 is true. If a linear transformation from a vector space to itself is injective, then it's also surjective, and thus a bijection. This is a fundamental result in linear algebra. So the final answer is: D. 'False, True'.

\*\*\*\*\*

Answer Option 2:

Statement 1 is false. If the dimension of the domain ( $V$ ) of a linear transformation is less than the dimension of the codomain ( $W$ ), then the linear transformation can be either injective or not. An example of non-injectivity (not one-to-one) is the zero transformation.

Statement 2 is true. If a linear transformation from a vector space to itself is injective, then it is also surjective (onto), and hence it is a bijection. This is a result from linear algebra known as the Rank-Nullity theorem.

Final answer: D

\*\*\*\*\*

Answer Option 3:

Statement 1: If  $\dim(V) < \dim(W)$ , then it's possible that  $T$  does not cover the entire space  $W$ . Therefore,  $T$  can't be injective. This statement is False.

Statement 2: If  $T: V \rightarrow V$  is linear and injective, it must be surjective (thus, a bijection) since its kernel is trivial (contains only the zero vector) and the dimension of the image equals the dimension of the original space. This statement is True.

Final Answer: D

\*\*\*\*\*

Answer Option 4:

Statement 1 | If  $T: V \rightarrow W$  is a linear transformation and  $\dim(V) < \dim(W) < 1$ , then  $T$  must be injective.

This statement is false. If the dimension of the domain ( $V$ ) is less than that of the codomain ( $W$ ), this doesn't necessarily mean that the linear transformation is injective.

Statement 2 | Let  $\dim(V) = n$  and suppose that  $T: V \rightarrow V$  is linear. If  $T$  is injective, then it is a bijection.

This statement is true. A linear transformation  $T: V \rightarrow V$  is a bijection if it's injective (or surjective), given that the dimensions of the domain and codomain are the same.

The final answer is D. 'False, True'

\*\*\*\*\*

Answer Option 5:

Statement 1 is False. If the dimension of  $V$  is less than the dimension of  $W$ , the linear transformation  $T$  could still fail to be injective. For example, it could map multiple vectors in  $V$  to the same vector in  $W$ , which would make it not injective.

Statement 2 is True. In a finite-dimensional vector space, injectivity implies surjectivity, and vice versa. So if  $T$  is a linear transformation from  $V$  to itself and it is injective, it must also be surjective, making it a bijection.

So, the final answer is D. 'False, True'

\*\*\*\*\*

Answer Option 6:

Statement 1: If the dimension of the domain of a linear transformation ( $V$ ) is less than the dimension of the codomain ( $W$ ), then the transformation can indeed be injective (one-to-one). However, the statement says that the dimension of  $W$  is less than 1, which means  $W$  should be a zero-dimension space. In this case,  $T$  cannot be injective unless  $V$  is also zero-dimension. Hence, the statement is false.

Statement 2: A linear transformation from a vector space to itself ( $T: V \rightarrow V$ ) that is injective is indeed also surjective, and thus bijective. This is because for finite-dimensional vector spaces, injectivity, surjectivity, and bijectivity are equivalent for linear transformations. Thus, the statement is true.

So, the final answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 7:

Statement 1: If  $\dim(V) < \dim(W) < 1$ , then  $\dim(V) = \dim(W) = 0$  (since dimension is non-negative and an integer). Hence,  $V$  and  $W$  must be the zero vector space. Any linear transformation  $T: V \rightarrow W$  in this case is injective. So, Statement 1 is True.

Statement 2:  $T$  being injective means that for any vectors  $v_1, v_2$  in  $V$ , if  $T(v_1) = T(v_2)$ , then  $v_1 = v_2$ . Since  $\dim(V) = n$  and  $T: V \rightarrow V$  is linear, if  $T$  is injective, then it must also be surjective, and thus bijective.

So, Statement 2 is True.

Final Answer: A. 'True, True'

\*\*\*\*\*

Answer Option 8:

Statement 1 is false. If  $\dim(V) < \dim(W)$ ,  $T$  can still fail to be injective. An injective function is one where each input is mapped to a unique output. Even if the dimension of  $V$  is less than that of  $W$ , it's possible for multiple vectors in  $V$  to be mapped to the same vector in  $W$ , causing  $T$  to be non-injective.

Statement 2 is true. In a linear transformation, if  $T: V \rightarrow V$  is injective (one-one), then it must be surjective (onto), and hence it is bijective. This is because, in finite dimensions, the rank-nullity theorem states that the sum of the dimension of the kernel (null space) and the rank (image) equals the dimension of the domain. If  $T$  is injective, then its kernel is  $\{0\}$ , so the dimension of the image must equal the dimension of the domain, implying that  $T$  is surjective.

So the final answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 9:

Statement 1: If  $T: V \rightarrow W$  is a linear transformation and  $\dim(V) < \dim(W) < 1$ , then  $T$  must be injective. This statement is False. A linear transformation from a vector space of lesser dimension to a vector space of higher dimension can never be injective.

Statement 2: Let  $\dim(V) = n$  and suppose that  $T: V \rightarrow V$  is linear. If  $T$  is injective, then it is a bijection. This statement is True. For linear transformations from a vector space to itself, being injective is equivalent to being surjective, and a transformation that is both injective and surjective is a bijection.

So the final answer is: D. 'False, True'

\*\*\*\*\*

Question 36:

'Find the degree for the given field extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$ .' A. '0', B. '4', C. '2', D. '6'

=====

Answer Option 1:

The field extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$  can be simplified as  $\mathbb{Q}(\sqrt{2} + \sqrt{3})$  over  $\mathbb{Q}$ . The minimal polynomial of  $\sqrt{2} + \sqrt{3}$  over  $\mathbb{Q}$  is  $x^4 - 10x^2 + 1$ , which has degree 4. Therefore, the degree of the field extension is 4. Final answer: B.

\*\*\*\*\*

Answer Option 2:

The extension field  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  contains  $\mathbb{Q}(\sqrt{2})$  and  $\mathbb{Q}(\sqrt{3})$ . Each of these is a quadratic extension of  $\mathbb{Q}$ , and  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  is the compositum of these two quadratic extension fields. Thus, the degree of the extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$  is at most  $2 \cdot 2 = 4$ . However, since  $\sqrt{2}$  and  $\sqrt{3}$  are not conjugate over  $\mathbb{Q}$ , the degree of the extension is exactly 4. Final Answer: B

\*\*\*\*\*

Answer Option 3:

The degree of the field extension is the dimension of the larger field when viewed as a vector space over the smaller field. The field  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  can be viewed as a  $\mathbb{Q}$ -vector space with basis  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ , so its dimension—and hence the degree of the extension—is 4. Final answer: B.

\*\*\*\*\*

Answer Option 4:

The degree of the field extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$  is 4. Consider the tower of extensions  $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ . The degree of  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}(\sqrt{2})$  is 2 because  $\sqrt{3}$  is not in  $\mathbb{Q}(\sqrt{2})$ , and the minimal polynomial of  $\sqrt{3}$  over  $\mathbb{Q}(\sqrt{2})$  is  $x^2 - 3$ . Similarly, the degree of  $\mathbb{Q}(\sqrt{2})$  over  $\mathbb{Q}$  is 2, so by the multiplicative property of degrees of extensions, the degree of  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$  is  $2 \cdot 2 = 4$ . Final Answer: B.

\*\*\*\*\*

Answer Option 5:

The degree of the extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$  is 4. To see this, note that  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  is the smallest field containing  $\mathbb{Q}$ ,  $\sqrt{2}$ , and  $\sqrt{3}$ . It is contained in the field  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6})$ , which is a vector space of dimension 4 over  $\mathbb{Q}$  with basis  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ . Since  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  contains 1,  $\sqrt{2}$ ,  $\sqrt{3}$ , and  $\sqrt{2}\sqrt{3} = \sqrt{6}$ , it must be exactly  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6})$ , and hence is a vector space of dimension 4 over  $\mathbb{Q}$ . Final Answer: B

\*\*\*\*\*

Answer Option 6:

The extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$  can be expressed as  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}(\sqrt{2})$  and  $\mathbb{Q}(\sqrt{2}) / \mathbb{Q}$ . The degree of the first extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}(\sqrt{2})$  is 2, because  $\sqrt{3}$  can be expressed as a linear combination of 1 and  $\sqrt{2}$ . Similarly, the degree of the second extension  $\mathbb{Q}(\sqrt{2}) / \mathbb{Q}$  is also 2, because  $\sqrt{2}$  can be expressed as a linear combination of 1 and  $\sqrt{3}$ . Therefore, the degree of the total extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$  is  $2 \cdot 2 = 4$ . Final answer: B.

\*\*\*\*\*

Answer Option 7:

The degree of the field extension is equal to the dimension of  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  as a vector space over  $\mathbb{Q}$ . To determine this, we need to find a basis for  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$ .

Notice that  $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$  are all elements of  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ , and they are linearly independent over  $\mathbb{Q}$ . Therefore, they form a basis for  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$ .

Since there are four elements in the basis, the degree of the field extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$  is 4.

So, the final answer is B. '4'.

\*\*\*\*\*

Answer Option 8:

The degree of field extension refers to the dimension of the larger field as a vector space over the smaller field.

Firstly,  $\mathbb{Q}(\sqrt{2})$  over  $\mathbb{Q}$  is a degree 2 extension, because  $\{1, \sqrt{2}\}$  forms a basis for  $\mathbb{Q}(\sqrt{2})$  over  $\mathbb{Q}$ .

Then, we consider  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}(\sqrt{2})$ . If  $\sqrt{3}$  were in  $\mathbb{Q}(\sqrt{2})$ , then  $(\sqrt{3})^2 = 3$  would be in  $\mathbb{Q}(\sqrt{2})$ , contradicting the fact that  $\mathbb{Q}(\sqrt{2})$  is a degree 2 extension of  $\mathbb{Q}$ . Therefore,  $\{1, \sqrt{3}\}$  forms a basis for  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}(\sqrt{2})$ , and thus  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}(\sqrt{2})$  is a degree 2 extension.

By the Tower Law, the degree of  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$  is then  $2 \cdot 2 = 4$ .

Final answer: B. '4'

\*\*\*\*\*

Answer Option 9:

We will use the multiplication rule for degrees of field extensions. This rule states that for fields  $F \subseteq K \subseteq L$ , we have that  $[L:F] = [L:K][K:F]$ .

In our case, we can take  $K = \mathbb{Q}(\sqrt{2})$  and  $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ . It is not hard to see that  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ , because  $\sqrt{3}$  is a root of the polynomial  $x^2 - 3$ , which is irreducible over  $\mathbb{Q}(\sqrt{2})$  by the Eisenstein Criterion for the prime  $p=3$ .

Also, observe that  $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ , because otherwise we would have that  $\sqrt{3} = a + b\sqrt{2}$  for some  $a, b \in \mathbb{Q}$ , and squaring gives  $3 = a^2 + 2b^2 + 2ab\sqrt{2}$ .

Since  $\mathbb{Q}(\sqrt{2})$  is a field, we know that  $2ab=0$ , meaning either  $a=0$  or  $b=0$ , but neither of these cases gives that  $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ .

Now, if we consider the polynomial  $f(x) = x^2 - 3 \in \mathbb{Q}(\sqrt{2})[x]$ , it is easy to see that it is irreducible (because its roots are  $\pm\sqrt{3}$ , which are not in  $\mathbb{Q}(\sqrt{2})$ ), and so  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ .

Then by the multiplication rule, we have that  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$ .

Therefore, the degree of the field extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$  is  $\boxed{4}$ . Final Answer: B  
\*\*\*\*\*

Question 37:

'Compute the product in the given ring.  $(20)(-8)$  in  $\mathbb{Z}_{26}$ , A. '0', B. '1', C. '11', D. '22'

=====

Answer Option 1:

We find the product in the integers and then reduce modulo 26. We get  $20 \times -8 = -160$ . Reducing modulo 26, we get  $-160 \equiv \boxed{22} \pmod{26}$ . Final answer: D

\*\*\*\*\*

Answer Option 2:

The product in the ring is simply the ordinary product, reduced modulo 26. So  $(20)(-8)$  in  $\mathbb{Z}_{26}$  is equivalent to  $(-160) \pmod{26}$ , which is 12. None of the given options match this answer. There seems to be an error in the provided options.

\*\*\*\*\*

Answer Option 3:

In the ring  $\mathbb{Z}_{26}$ , the product of two numbers is just their product as integers, reduced modulo 26. Hence,  $(20)(-8) = -160 \equiv \boxed{8} \pmod{26}$ .

However, as the options do not contain this answer, it seems there might be a miscommunication or mistake in the problem or the options.

\*\*\*\*\*

Answer Option 4:

When computing products in the ring  $\mathbb{Z}_n$ , you perform the multiplication as usual, but then take your product mod  $n$ . So, in  $\mathbb{Z}_{26}$ ,  $(20)(-8) = -160$ . Then,  $-160 \equiv \boxed{18} \pmod{26}$ . None of the given answers are correct.

\*\*\*\*\*

Answer Option 5:

The product of 20 and -8 in the ring  $\mathbb{Z}_{26}$  is  $(20)(-8) = -160 = 18 \pmod{26}$ . This is not an answer choice, but since  $18 \equiv -8 \pmod{26}$ , we have that -8 is the correct answer. We see that option A is equal to -8 in mod 26, so the final answer is  $\boxed{0}$ . Final Answer: A

\*\*\*\*\*

Answer Option 6:

First multiply 20 by -8 to get -160. We then want to find the residue of -160 modulo 26.

Add 160 to 26 repeatedly until a number between 0 and 25 is found, that's 6. Therefore,  $(20)(-8)$  in  $\mathbb{Z}_{26}$  equals 6. But none of the options matches this result. Please check your options again.

\*\*\*\*\*

Answer Option 7:

We can compute this product by normal multiplication, getting  $20 \times -8 = -160$ . Then, to find this number modulo 26, we note that  $-160 \equiv 6 \pmod{26}$ . So  $(20)(-8) \equiv 6 \pmod{26}$  in the ring  $\mathbb{Z}_{26}$ .

However, none of the given options match this result. There might be a mistake in the problem or the options.

\*\*\*\*\*

Answer Option 8:

In  $\mathbb{Z}_{26}$ , the product of 20 and -8 is congruent to  $20 \cdot (-8)$ . So,  $(20)(-8) = -160$ . In  $\mathbb{Z}_{26}$ , this means we need to find an integer  $k$  such that  $26k$  is between -160 and -160+26. Since  $-160 = -7 \cdot 26 + 2$ , the equivalence class of -160 in  $\mathbb{Z}_{26}$  is 2. So,  $(20)(-8)$  is '2'. However, since the given options do not include '2', it seems there might be a mistake.

\*\*\*\*\*

Answer Option 9:

To compute the product, first multiply  $20$  and  $-8$  to get  $-160$ . Then, calculate  $-160 \pmod{26}$  to find the equivalent class in  $\mathbb{Z}_{26}$ . This gives  $-160 \pmod{26} = 22$  because the integer  $-160$  is  $22$  more than a multiple of  $26$  ( $-160 = -6(26) + 22$ ). Thus, the product of  $20$  and  $-8$  in  $\mathbb{Z}_{26}$  is  $\boxed{22}$ . Final answer: D

\*\*\*\*\*

Question 38:

Determine whether the polynomial in  $\mathbb{Z}[x]$  satisfies an Eisenstein criterion for irreducibility over  $\mathbb{Q}$ .  $x^2 - 12$ , A. 'Yes, with  $p=2$ .' B. 'Yes, with  $p=3$ .' C. 'Yes, with  $p=5$ .' D. 'No.'

=====

Answer Option 1:

The Eisenstein criterion requires a prime number  $p$  such that  $p$  divides all coefficients except for the leading coefficient,  $p^2$  does not divide the constant coefficient, and  $p$  does not divide the leading coefficient.

For the polynomial  $x^2 - 12$ , we see that neither 2, 3, nor 5 satisfies these conditions. Thus, the answer is 'No.' Final Answer: D.

=====

Answer Option 2:

The Eisenstein criterion states that if there is a prime number  $p$  such that  $p$  divides all coefficients except the leading coefficient,  $p^2$  does not divide the constant term, and  $p$  does not divide the leading coefficient, then the polynomial is irreducible over rational numbers.

Consider the polynomial  $x^2 - 12$ . The coefficients are 1, 0 and -12. No prime number divides both 0 and -12 without also dividing 1. Hence, we cannot apply the Eisenstein criterion. The answer is

$\boxed{\text{No.}}$

=====

Answer Option 3:

An Eisenstein criterion for irreducibility over  $\mathbb{Q}$  is that there exists a prime number  $p$  such that  $p$  divides all coefficients of the polynomial except the leading one,  $p^2$  does not divide the constant term, and  $p$  does not divide the leading coefficient.

For the given polynomial  $x^2 - 12$ , the coefficients are 1 and -12. There is no prime number satisfying the Eisenstein criterion since 1 is not divisible by any prime and the only primes dividing 12 are 2 and 3, but  $2^2$  (4) and  $3^2$  (9) both divide 12.

So, the answer is D. 'No.'

=====

Answer Option 4:

Eisenstein's criterion states that a polynomial is irreducible over  $\mathbb{Q}$  if there exists a prime number  $p$  such that  $p$  divides all coefficients except the leading one,  $p$  does not divide the leading coefficient, and  $p^2$  does not divide the constant term. In the polynomial  $x^2 - 12$ , the coefficients are 1 and -12. The leading coefficient 1 is not divisible by any prime, and -12 is divisible by the primes 2 and 3, but  $2^2$  and  $3^2$  do not divide -12. Therefore, the polynomial does not satisfy Eisenstein's criterion. So, the answer is 'No.' Final Answer: D

=====

Answer Option 5:

According to the Eisenstein criterion, a polynomial is irreducible over  $\mathbb{Q}$  if there exists a prime number  $p$  such that  $p$  divides all the coefficients of the polynomial except the leading coefficient,  $p$  does not divide the leading coefficient, and  $p^2$  does not divide the constant term. In the polynomial  $x^2 - 12$ , the coefficients are 1 and -12. There is no prime number that divides -12 but does not divide 1, and the square of which does not divide -12. So the polynomial does not satisfy the Eisenstein criterion. Final Answer: D. 'No.'

=====

Answer Option 6:

The Eisenstein criterion states that a polynomial is irreducible if we can find a prime number  $p$  such that  $p$  divides all coefficients except the leading coefficient,  $p^2$  does not divide the constant term, and  $p$  does not divide the leading coefficient.

In the polynomial  $x^2 - 12$ , there's no prime number  $p$  such that  $p$  divides both coefficients (1 and -12) but  $p^2$  does not divide the constant term (-12). Therefore, the polynomial does not satisfy the Eisenstein criterion. The answer is D. 'No.'

=====

Answer Option 7:

The Eisenstein criterion for irreducibility over  $\mathbb{Q}$  states that a polynomial of the form  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  is irreducible if there is some prime  $p$  such that  $p \mid a_i$  for all  $i < n$ ,  $p^2 \nmid a_0$ , and  $p \nmid a_n$ . In this case, our polynomial is  $x^2 - 12$ . We can see that 2, 3, and 5 do not divide the leading coefficient  $a_n = 1$ , and thus they cannot serve as the prime  $p$  in the Eisenstein criterion. Therefore, the polynomial does not satisfy an Eisenstein criterion for irreducibility over  $\mathbb{Q}$ , and our final answer is D.

=====

Answer Option 8:

An Eisenstein criterion states that a polynomial of the form  $x^n + p_1 x^{n-1} + \dots + p_{n-1} x + p_n$  is irreducible over  $\mathbb{Q}$  if a prime number  $p$  exists such that  $p$  divides all  $p_i$  for  $1 \leq i < n$ ,  $p$  does not divide  $p_n$ , and  $p^2$  does not divide  $p_n$ . The given polynomial  $x^2 - 12$ , only the constant term -12 has a coefficient divisible by a prime number. In this case, the primes are 2 and 3. However, the coefficient of  $x$ , which is 0, is divisible by any prime number, which means there's no prime number  $p$  that will satisfy the requirements of the Eisenstein criterion. Therefore, the polynomial does not satisfy the Eisenstein criterion. The answer is D. 'No.'

=====

Answer Option 9:

The Eisenstein's criterion states that a polynomial of the form  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  is irreducible if there exists a prime number  $p$  such that  $p$  does not divide  $a_n$ ,  $p$  divides  $a_i$  for  $0 \leq i < n$ , and  $p^2$  does not divide  $a_0$ .

The polynomial  $x^2 - 12$  can be rewritten as  $x^2 - 2^2 \cdot 3$ . No prime number divides both coefficients (1 and -12) and the square of no prime number divides the constant term -12. Therefore, the polynomial does not satisfy Eisenstein's criterion.



Final answer: D. 'No.'

\*\*\*\*\*

Question 39:

'Find the generator for the finite field  $\mathbb{Z}_7$ ;', A. '1', B. '2', C. '3', D. '4'

=====

Answer Option 1:

The generator of the finite field  $\mathbb{Z}_7$  is 3, which when raised to different powers (modulo 7), can generate all non-zero elements of the field  $\mathbb{Z}_7$ . So, the correct final answer is C. '3'.

\*\*\*\*\*

Answer Option 2:

A generator for the finite field  $\mathbb{Z}_7$  is '3'. When repeatedly multiplied by itself modulo 7, 3 generates all non-zero elements in the field:  $3^1 = 3$ ,  $3^2 = 2$ ,  $3^3 = 6$ ,  $3^4 = 4$ ,  $3^5 = 5$ ,  $3^6 = 1 \pmod{7}$ . Hence, the correct answer is C. '3'.

\*\*\*\*\*

Answer Option 3:

A generator for a finite field is an element which can be used to generate all other non-zero elements of the field by taking powers of the generator. In the field  $\mathbb{Z}_7$ , 3 is a generator because  $3^1=3$ ,  $3^2=2$ ,  $3^3=6$ ,  $3^4=4$ ,  $3^5=5$ , and  $3^6=1$ , which are all the non-zero elements of  $\mathbb{Z}_7$ . So, the answer is C. '3'.

\*\*\*\*\*

Answer Option 4:

The generator for a finite field  $\mathbb{Z}_p$  is a number  $g$  such that every non-zero element of the field can be written as  $g^n$  for some non-negative integer  $n$ . In other words, the generator  $g$  generates the multiplicative group of the field under multiplication.

For the field  $\mathbb{Z}_7$  (which consists of the elements 0, 1, 2, 3, 4, 5, 6 under addition and multiplication modulo 7), the generator is 3. This is because  $3^n \pmod{7}$  produces all non-zero elements of the field as  $n$  ranges from 1 to 6. Specifically,  $3^1 = 3$ ,  $3^2 = 2$ ,  $3^3 = 6$ ,  $3^4 = 4$ ,  $3^5 = 5$ , and  $3^6 = 1 \pmod{7}$ .

So, the generator for the finite field  $\mathbb{Z}_7$  is 3. Final answer: C.

\*\*\*\*\*

Answer Option 5:

The generator of a finite field is an element that can generate all the non-zero elements (1 to  $n-1$ , where  $n$  is the field size) of the field by taking powers of it. Here, we are working with field  $\mathbb{Z}_7$  so we need to find an element such that its powers modulo 7 can generate 1, 2, 3, 4, 5 and 6.

If we consider element '3', we have:

$$3^1 = 3 \pmod{7},$$

$$3^2 = 9 \pmod{7} = 2,$$

$$3^3 = 27 \pmod{7} = 6,$$

$$3^4 = 81 \pmod{7} = 4,$$

$$3^5 = 243 \pmod{7} = 5,$$

$$3^6 = 729 \pmod{7} = 1 \text{ (Fermat's little theorem)}$$

So, '3' can generate all the non-zero elements of the field  $\mathbb{Z}_7$ . Therefore, final answer is C. '3' is the generator for the finite field  $\mathbb{Z}_7$ .

\*\*\*\*\*

Answer Option 6:

A generator for the finite field  $\mathbb{Z}_7$  is an element that, when raised to different powers, produces all the non-zero elements of the field.  $\mathbb{Z}_7$  is the set  $\{0, 1, 2, 3, 4, 5, 6\}$ .

Let's check each of the options:

- A. Raising 1 to any power just gives 1, so it cannot generate all non-zero elements.
- B. Raising 2 to different powers modulo 7 gives us  $\{2, 4, 1, 2, 4, 1, \dots\}$ , so it does generate all non-zero elements.
- C. Raising 3 to different powers modulo 7 gives us  $\{3, 2, 6, 4, 5, 1, \dots\}$ , so it does generate all non-zero elements.
- D. Raising 4 to different powers modulo 7 gives us  $\{4, 2, 1, 4, 2, 1, \dots\}$ , so it does generate all non-zero elements.

Therefore, the generator for the finite field  $\mathbb{Z}_7$  is any one of these answers: B, C, or D. However, since the question asks for only one answer, we choose the smallest non-zero generator which is

$\boxed{2}$ . Final answer: B.

\*\*\*\*\*

Answer Option 7:

A generator for a finite field  $\mathbb{Z}_p$  is a number  $g$  such that for every non-zero  $x$  in  $\mathbb{Z}_p$ , there exists an integer  $n$  such that  $g^n = x \pmod{p}$ .

In this problem, we are looking for a generator for  $\mathbb{Z}_7$ , which means we need to find a number  $g$  such that for every  $x$  in  $\{1, 2, 3, 4, 5, 6\}$ , there exists an integer  $n$  such that  $g^n = x \pmod{7}$ .

We can check each of the options:

- A. '1' is not a generator, because for any  $n$ ,  $1^n = 1 \pmod{7}$ .
- B. '2' is a generator, because the powers of 2 mod 7 are  $\{2, 4, 1, 2, 4, 1, \dots\}$ , which includes all non-zero elements of  $\mathbb{Z}_7$ .
- C. '3' is not a generator, because the powers of 3 mod 7 are  $\{3, 2, 6, 4, 5, 1, 3, \dots\}$ , which includes all non-zero elements of  $\mathbb{Z}_7$ .
- D. '4' is not a generator, because the powers of 4 mod 7 are  $\{4, 2, 1, 4, 2, 1, \dots\}$ , which does not include all non-zero elements of  $\mathbb{Z}_7$ .

Therefore, the generator for the finite field  $\mathbb{Z}_7$  is '2'. Final Answer: B

\*\*\*\*\*

Answer Option 8:

A generator for a finite field  $\mathbb{Z}_p$  is an element  $g$  such that every non-zero element of the field can be written as a power of  $g$ . This means that  $g, g^2, g^3, \dots, g^{(p-1)}$  are distinct and cover all the non-zero elements of the field.

In the case of  $\mathbb{Z}_7$ , we can check each of the options:

A. '1' is not a generator because  $1^k$  is always 1, regardless of  $k$ .

B. '2' is a generator because  $2, 2^2 = 4, 2^3 = 1 \pmod{7}, 2^4 = 2, 2^5 = 4, 2^6 = 1$  cover all the non-zero elements of  $\mathbb{Z}_7$ .

C. '3' is not a generator because  $3^2 = 2 \pmod{7}, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$  does not cover all the non-zero elements of  $\mathbb{Z}_7$ .

D. '4' is not a generator because  $4^2 = 2 \pmod{7}, 4^3 = 1, 4^4 = 4, 4^5 = 2, 4^6 = 1$  does not cover all the non-zero elements of  $\mathbb{Z}_7$ .

So the answer is B. '2'.

\*\*\*\*\*

Answer Option 9:

A generator for a finite field is an element such that any non-zero element of the field can be expressed as a power of the generator. The field  $\mathbb{Z}_7$  has elements  $\{0, 1, 2, 3, 4, 5, 6\}$ .

We need to find an element  $g$  such that  $\{1, g, g^2, g^3, g^4, g^5, g^6\}$  is a permutation of  $\{1, 2, 3, 4, 5, 6\}$ .

Let's check the options:

A.  $1^1 = 1, 1^2 = 1, 1^3 = 1, 1^4 = 1, 1^5 = 1, 1^6 = 1$ . This is not a permutation of  $\{1, 2, 3, 4, 5, 6\}$ .

B.  $2^1 = 2, 2^2 = 4, 2^3 = 1, 2^4 = 2, 2^5 = 4, 2^6 = 1$ . This is not a permutation of  $\{1, 2, 3, 4, 5, 6\}$ .

C.  $3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$ . This is a permutation of  $\{1, 2, 3, 4, 5, 6\}$ .

D.  $4^1 = 4, 4^2 = 2, 4^3 = 1, 4^4 = 4, 4^5 = 2, 4^6 = 1$ . This is not a permutation of  $\{1, 2, 3, 4, 5, 6\}$ .

Therefore, the generator for the finite field  $\mathbb{Z}_7$  is 3. Final Answer: C

\*\*\*\*\*

Question 40:

'Statement 1 | Every permutation is a cycle. Statement 2 | Every cycle is a permutation.', A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

A permutation is a rearrangement of elements in a set. A cycle is a type of permutation that moves elements around in a cyclic manner. Therefore, while every cycle is a permutation, not every permutation is a cycle, since some permutations can involve more complex rearrangements that can't be described as a single cycle. Therefore, Statement 1 is False and Statement 2 is True. Final answer: D.

\*\*\*\*\*

Answer Option 2:

Statement 1 is False. Not every permutation is a cycle. For example, the permutation (1 3)(2 4) is not a cycle.

Statement 2 is True. Every cycle is a permutation. A cycle is a specific kind of permutation where only a subset of the elements are permuted cyclically.

So, the correct answer is D. 'False, True'

\*\*\*\*\*

Answer Option 3:

A permutation is a rearrangement of objects in a set. A cycle is a special subset of permutations where a subset of the objects are rotated amongst themselves, leaving the other objects fixed. Thus, while every cycle is indeed a permutation (Statement 2: True), it is incorrect to say every permutation is a cycle, as there are also many permutations that are not cycles (Statement 1: False). Final Answer: D.

'False, True'

\*\*\*\*\*

Answer Option 4:

A permutation is a rearrangement of items into a particular order. A cycle is a particular type of permutation where a number of elements are cyclically permuted. Therefore, Statement 1 is false because while every cycle is a permutation, not every permutation is a cycle. Statement 2 is indeed true because a cycle is a particular type of permutation. So, the final answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 5:

Statement 1 is false. Not every permutation is a cycle. For example, consider the permutation (1 2)(3 4) of {1,2,3,4}. This is a permutation but it's not a cycle because it can't be expressed as a single cycle.

Statement 2 is true. Every cycle is a permutation. A cycle is simply a type of permutation where we cyclically permute some elements in a set, leaving the rest fixed.

So, the correct answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 6:

Statement 1: Every permutation is a cycle. This statement is false. A permutation is an arrangement of objects in a definite order. The selection of objects is taken from a collection or a set without regards to the order of arrangement. A cycle refers to a permutation where only a subset of the elements are permuted, and the rest are kept fixed. Therefore, not all permutations are cycles.

Statement 2: Every cycle is a permutation. This statement is true. As described earlier, a cycle is a certain type of permutation where only a subset of the elements are permuted. Hence, all cycles are indeed permutations.

Final answer: D. 'False, True'

\*\*\*\*\*

Answer Option 7:

A permutation is a rearrangement of the elements of a set. A cycle is a type of permutation in which a subset of the elements are cyclically permuted.

Statement 1: Every permutation is a cycle. This statement is False. Not every permutation is a cycle. For example, consider the permutation of (1,2,3) to (3,1,2). This is not a simple cycle.

Statement 2: Every cycle is a permutation. This statement is True. Every cycle is indeed a permutation, because it is a particular way of rearranging a subset of the elements of a set.

So, the final answer is: D. 'False, True'

\*\*\*\*\*

Answer Option 8:

Statement 1 is false. Not every permutation is a cycle. For example, consider the permutation of the set {1, 2, 3} that maps 1 to 2, 2 to 3, and 3 to 1. This is a cycle (specifically, a 3-cycle). However, the permutation that maps 1 to 1, 2 to 3, and 3 to 2 is not a cycle, because it consists of a 1-cycle and a 2-cycle.

Statement 2 is true. Every cycle is a permutation. A cycle is a special type of permutation in which only a subset of the elements are permuted in a cyclic manner.

So, the final answer is D, 'False, True'.

\*\*\*\*\*

Answer Option 9:

A permutation is an arrangement of objects in a specific order. The order of arrangement of the object is very crucial. The number of permutations on a set of n elements is given by n! (n factorial).

A cycle in permutations refers to the cyclic nature of a permutation, where the positions of the elements cycle in a circular manner.

As for the statements:

Statement 1 | Every permutation is a cycle.

This statement is False. While it's true that many permutations can be expressed as a product of cycles, not every permutation is a cycle.

Statement 2 | Every cycle is a permutation.

This statement is True. A cycle is a specific type of permutation, where some or all of the elements in a set are moved in a cyclic pattern.

So the correct answer is D. 'False, True'

\*\*\*\*\*

Question 41:

The set of integers  $\mathbb{Z}$  with the binary operation  $***$  defined as  $a*b = a + b + 1$  for  $a, b$  in  $\mathbb{Z}$ , is a group. The identity element of this group is', A. '0', B. '1', C. '-1', D. '12'

=====

Answer Option 1:

The identity element of a group is the element that, when combined with any element of the group using the group operation, does not change that element.

Let 'e' be the identity element of this group. Then for any integer 'a' in  $\mathbb{Z}$ ,

$$a * e = a + e + 1 = a$$

Solving for e, we get  $e = -1$

So the identity element of this group is '-1'. Final Answer: C.

=====

Answer Option 2:

For an element e to be the identity, we must have  $a * e = a$  and  $e * a = a$  for all a in  $\mathbb{Z}$ . From the definition of  $*$ , this means  $a + e + 1 = a$  and  $e + a + 1 = a$ . Simplifying both equations gives  $e + 1 = 0$ , so the identity element e is -1. Hence, the correct answer is C. '-1'.

=====

Answer Option 3:

The identity element in a group is the element that leaves other elements unchanged when the group's operation is applied. In other words, for any integer  $a$ , we want to find an integer  $e$  such that  $a * e = a + e + 1 = a$ . Solving for  $e$ , we get  $e = -1$ . Thus, the identity element of the group is  $\boxed{-1}$ . Final Answer: C

=====

Answer Option 4:

The identity element  $e$  for a group is the element such that for every element  $a$  in the group,  $a * e = e * a = a$ .

Therefore, we need to find  $e$  such that  $a + e + 1 = a$  and  $e + a + 1 = a$ .

Solving these equations gives  $e = -1$ , so the identity element is  $\boxed{-1}$ .

Final Answer: C

=====

Answer Option 5:

The identity element  $e$  in a group is the one that, when combined with any element  $a$  in the group via the binary operation, gives  $a$ . In other words,  $a * e = e * a = a$  for all  $a$  in the group.

Let's set up the equation  $a * e = a$ , for any integer  $a$ . Substituting the given operation, we get  $a + e + 1 = a$ .

Solving for  $e$ , we find  $e = -1$ . Therefore, the identity element of this group is  $\boxed{-1}$ . Final Answer: C

=====

Answer Option 6:

The identity element of a group is the element that, when combined with any element of the group using the group operation, does not change that element. If 'e' is the identity, we should have  $a * e = e * a = a$  for any 'a' in the group. For this problem, we should have  $a * e = a + e + 1 = a$  and  $e * a = e + a + 1 = a$ . Solving these equations gives  $e = -1$ . So, the identity element of this group is -1. Final answer: C.

=====

Answer Option 7:

The identity element of a group is the element that, when combined with any other element using the group's operation, does not change that element. In other words, if 'e' is the identity element, then for all  $a$  in  $\mathbb{Z}$ ,  $a * e = a$  and  $e * a = a$ . Using the definition of the operation  $*$ , we get  $a + e + 1 = a$  and  $e + a + 1 = a$ , which simplifies to  $e + 1 = 0$ . Therefore,  $e = -1$ , so the identity element of the group is '-1'. Final answer: C.

=====

Answer Option 8:

In a group, the identity element  $e$  is the one that, combined with any element  $a$  in the group under the group operation (in this case  $***$ ), leaves  $a$  unchanged. Symbolically, this is:  $e * a = a$  and  $a * e = a$ . In the case of the given binary operation  $***$ , the identity element  $e$  must satisfy the following for all  $a$  in the integers:  $e * a = e + a + 1 = a$  and  $a * e = a + e + 1 = a$ . Solving either of these equations for  $e$  gives  $e = -1$ . Hence, the identity element of this group is  $\boxed{-1}$ . Final answer: C.

=====

Answer Option 9:

The identity element  $e$  of a group is the one that satisfies the property  $a * e = a$  and  $e * a = a$  for all  $a$  in the group. In this case, we want to find an  $e$  such that  $a * e = a + e + 1 = a$  and  $e * a = e + a + 1 = a$ .

Solving the equation  $a + e + 1 = a$ , we find that  $e = -1$ . Also, the equation  $e + a + 1 = a$  gives  $e = -1$ . Therefore, the identity element of this group is -1.

Final Answer: C. '-1'

=====

Question 42:

'Find the characteristic of the ring  $\mathbb{Z}_3 \times 3\mathbb{Z}$ .' A. '0', B. '3', C. '12', D. '30'

=====

Answer Option 1:

The characteristic of a ring is the smallest positive integer  $n$  such that  $n \cdot 1 = 0$  for every element  $1$  in the ring. In this case, the ring is  $\mathbb{Z}_3 \times 3\mathbb{Z}$ . The characteristic of  $\mathbb{Z}_3$  is  $3$  and the characteristic of  $3\mathbb{Z}$  is also  $3$ . The characteristic of the product ring is the least common multiple of these two characteristics, which is  $\boxed{3}$ . Final answer: B.

\*\*\*\*\*

Answer Option 2:

The characteristic of a ring is the smallest positive integer  $n$  such that  $na = 0$  for all  $a$  in the ring. If no such  $n$  exists, the characteristic is  $0$ .

The ring  $\mathbb{Z}_3$  has characteristic  $3$  because  $3$  times any element is  $0$ .

The ring  $3\mathbb{Z}$  also has characteristic  $3$  because  $3n$  is  $0$  for any  $n$  in  $3\mathbb{Z}$ .

Since the characteristic of both rings is  $3$ , the characteristic of the product ring  $\mathbb{Z}_3 \times 3\mathbb{Z}$  is also  $\boxed{3}$ . Final answer: B.

\*\*\*\*\*

Answer Option 3:

The characteristic of a ring is the smallest positive integer  $n$  such that for all elements  $a$  in the ring,  $na = 0$ . For  $\mathbb{Z}_3$ , any element times  $3$  is  $0$ , and in  $3\mathbb{Z}$ , any element times  $1$  is  $0$ . The characteristic of the ring  $\mathbb{Z}_3 \times 3\mathbb{Z}$  is the least common multiple of these two characteristics, which is  $3$ . So, the final answer is B. '3'.

\*\*\*\*\*

Answer Option 4:

The characteristic of a ring is the smallest positive integer  $n$  such that  $na = 0$  for all  $a$  in the ring, where  $na$  denotes the sum of  $n$  copies of  $a$ .

The ring  $\mathbb{Z}_3 \times 3\mathbb{Z}$  consists of ordered pairs  $(a, b)$ , where  $a \in \mathbb{Z}_3$  and  $b \in 3\mathbb{Z}$ .

We find that multiplying any element of  $\mathbb{Z}_3$  by  $3$  gives  $0$ , and multiplying any element of  $3\mathbb{Z}$  by  $1$  gives a nonzero value. Therefore, the characteristic of the ring  $\mathbb{Z}_3 \times 3\mathbb{Z}$  is  $\boxed{3}$ . Final Answer: B.

\*\*\*\*\*

Answer Option 5:

The characteristic of a ring is the smallest positive integer  $n$  such that  $n \cdot 1 = 0$ . In the ring  $\mathbb{Z}_3 \times 3\mathbb{Z}$ , the identity is  $(1, 0)$ . The smallest positive integer  $n$  such that  $n \cdot (1, 0) = (n, 0) = (0, 0)$  is  $3$ . Therefore, the characteristic of the ring  $\mathbb{Z}_3 \times 3\mathbb{Z}$  is  $\boxed{3}$ . Final answer: B

\*\*\*\*\*

Answer Option 6:

The characteristic of a ring is the smallest positive integer  $n$  such that  $n \cdot 1 = 0$ . If no such  $n$  exists, then the characteristic is  $0$ .

The ring  $\mathbb{Z}_3$  has characteristic  $3$  and the ring  $3\mathbb{Z}$  has characteristic  $0$  (since it is just the integers multiplied by  $3$ ).

The direct product of two rings,  $\mathbb{Z}_3$  and  $3\mathbb{Z}$ , denoted  $\mathbb{Z}_3 \times 3\mathbb{Z}$ , has characteristic equal to the least common multiple of the characteristics of  $\mathbb{Z}_3$  and  $3\mathbb{Z}$ .

Therefore, the characteristic of the ring  $\mathbb{Z}_3 \times 3\mathbb{Z}$  is  $\text{lcm}(3, 0) = \boxed{0}$ .

Final answer: A.

\*\*\*\*\*

Answer Option 7:

The characteristic of a ring  $R$ , denoted by  $\text{char}(R)$ , is defined as the smallest positive integer  $n$  such that  $n \cdot r = 0$  for every  $r$  in  $R$ . If no such positive integer exists, then the characteristic is defined to be  $0$ .

The ring  $\mathbb{Z}_3 \times 3\mathbb{Z}$  is the Cartesian product of the ring of integers modulo  $3$  and the ring of integers multiplied by  $3$ .

The characteristic of  $\mathbb{Z}_3$  is  $3$  because  $3 \cdot r = 0 \pmod 3$  for every  $r$  in  $\mathbb{Z}_3$ .

The characteristic of  $3\mathbb{Z}$  is  $1$  because  $1 \cdot r = 3r$  is still in  $3\mathbb{Z}$  for every  $r$  in  $3\mathbb{Z}$ .

The characteristic of a product of two rings is the least common multiple of the characteristics of the individual rings.

Therefore, the characteristic of  $\mathbb{Z}_3 \times 3\mathbb{Z}$  is  $\text{lcm}(3, 1) = 3$ .

Final answer: B

\*\*\*\*\*

Answer Option 8:

The characteristic of a ring is the smallest positive integer  $n$  such that  $na = 0$  for all elements  $a$  in the ring. If no such integer exists, the characteristic is  $0$ .

$\mathbb{Z}_3$  has characteristic  $3$  because  $3n = 0 \pmod 3$  for all integers  $n$ .  $3\mathbb{Z}$  (the integers multiple of  $3$ ) has characteristic  $3$  because  $3n = 0$  for all integers  $n$ .

The ring  $\mathbb{Z}_3 \times 3\mathbb{Z}$  consists of pairs  $(a, b)$  where  $a$  is in  $\mathbb{Z}_3$  and  $b$  is in  $3\mathbb{Z}$ . The operation is component-wise, so the characteristic is the smallest positive integer  $n$  such that  $n(a, b) = (0, 0)$ .

We know that  $na = 0$  in  $\mathbb{Z}_3$  for  $n=3$ , and  $nb = 0$  in  $3\mathbb{Z}$  for  $n=3$ , so  $n(a, b) = (0, 0)$  in  $\mathbb{Z}_3 \times 3\mathbb{Z}$  for  $n=3$ . Therefore, the characteristic of  $\mathbb{Z}_3 \times 3\mathbb{Z}$  is  $\boxed{3}$ . Final answer: B

\*\*\*\*\*

Answer Option 9:

The characteristic of a ring is the least positive integer  $n$  such that  $n \cdot 1_R = 0$ , where  $1_R$  is the multiplicative identity in the ring  $R$  and  $n \cdot 1_R$  denotes the result of adding  $1_R$  to itself  $n$  times. If no such positive integer exists, then the characteristic of the ring is  $0$ .

In the case of the ring  $\mathbb{Z}_3 \times \mathbb{Z}_3$ , we see that  $(1,1)$  is the multiplicative identity. Thus, we need to find the smallest positive integer  $n$  such that  $n \cdot (1,1) = (n \bmod 3, n \bmod 3) = (0,0)$ . This will occur when  $n$  is a multiple of 3, and  $3n$  is a multiple of  $3^2 = 9$ . The smallest such  $n$  is  $\boxed{9}$ .

However, this answer is not present in the options. It is likely there was a mistake in the problem or the options. If the ring was intended to be  $\mathbb{Z}_3 \times \mathbb{Z}_3$ , the characteristic would be 3, option B. If the ring was intended to be  $\mathbb{Z}_{12} \times \mathbb{Z}_{12}$ , the characteristic would be 12, option C. Unfortunately, without clarification, it's impossible to identify the intended correct answer.

\*\*\*\*\*



Question 43:

'Statement 1 | Some abelian group of order 45 has a subgroup of order 10. Statement 2 | A subgroup H of a group G is a normal subgroup if and only if the number of left cosets of H is equal to the number of right cosets of H.', A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1: False. An abelian group of order 45 must be the direct product of cyclic groups of order 5 and 9 (by the Fundamental Theorem of Finite Abelian Groups). It cannot therefore have a subgroup of order 10.

Statement 2: True. A subgroup H of a group G is a normal subgroup if and only if the set of left cosets of H equals the set of right cosets of H.

So the answer is: D. 'False, True'.

\*\*\*\*\*

Answer Option 2:

Statement 1 | False. Every abelian group of order 45 is isomorphic to either  $\mathbb{Z}_{45}$  or  $\mathbb{Z}_{15} \times \mathbb{Z}_3$ . Neither of these groups has a subgroup of order 10 (all subgroup orders must divide the group order by Lagrange's Theorem).

Statement 2 | True. A subgroup H of a group G is a normal subgroup if and only if the left cosets of H in G are precisely the right cosets of H in G.

Hence, the final answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 3:

Statement 1 is false. By the Fundamental Theorem of Finite Abelian Groups, every finite abelian group is isomorphic to a direct product of cyclic groups of prime power order, and a subgroup of order 10 cannot exist in a group of order  $45 = 3^2 \cdot 5$  because 2 is not a factor of 45.

Statement 2 is true. A subgroup H of a group G is a normal subgroup if and only if the number of left cosets of H is equal to the number of right cosets of H. This is by definition of a normal subgroup.

Hence, the correct answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 4:

Statement 1: Any group of order 45 is isomorphic to either  $\mathbb{Z}_{45}$  or  $\mathbb{Z}_9 \times \mathbb{Z}_5$ . Neither of these groups has a subgroup of order 10 (in fact, by Lagrange's theorem, the order of any subgroup must divide the order of the group), so the statement is False.

Statement 2: This is a standard result in group theory. The set of left cosets of a subgroup H in a group G forms a partition of G, as does the set of right cosets. A subgroup H is normal if and only if these two partitions coincide, i.e., if each left coset is also a right coset. So, the statement is True.

So, the correct option is D. 'False, True'

\*\*\*\*\*

Answer Option 5:

Statement 1 | False: An abelian group of order 45 has prime factors 3 and 5 only (since  $45 = 3^2 \cdot 5$ ). By the Fundamental Theorem of Finite Abelian Groups, this group must be isomorphic to one of the following groups:  $\mathbb{Z}_{45}$ ,  $\mathbb{Z}_9 \times \mathbb{Z}_5$ , or  $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ . None of these groups has a subgroup of order 10.

Statement 2 | True: This is a basic property of normal subgroups. A subgroup H of a group G is normal iff the left cosets of H in G are the same as the right cosets of H in G.

So, the final answer is D - 'False, True'.

\*\*\*\*\*

Answer Option 6:

Statement 1: False. By the fundamental theorem of finite abelian groups, any group of order 45 must be isomorphic to either  $\mathbb{Z}_{45}$  or  $\mathbb{Z}_9 \times \mathbb{Z}_5$ . In either case, every subgroup must have order dividing 45, and since 10 does not divide 45, there cannot be a subgroup of order 10.

Statement 2: True. By the definition of a normal subgroup,  $H$  is a normal subgroup of  $G$  if and only if  $gH = Hg$  for all  $g \in G$ . This is the same as the condition that the number of left cosets of  $H$  is the same as the number of right cosets.

So, the correct answer is  $\boxed{\text{D}} \text{ 'False, True'}$ .

\*\*\*\*\*

Answer Option 7:

Statement 1 is False. By the fundamental theorem of finite abelian groups, every abelian group of order 45 is isomorphic to a direct product of cyclic groups of order 3 and 5, and none of these has a subgroup of order 10.

Statement 2 is True. The number of left cosets of a subgroup H in a group G is always equal to the number of right cosets of H in G, regardless of whether H is a normal subgroup of G. This is a consequence of Lagrange's theorem, which states that the order of a subgroup divides the order of the group.

So the correct answer is D. 'False, True'.

\*\*\*\*\*

Answer Option 8:

Statement 1 is false. An abelian group of order 45 must be isomorphic to either  $\mathbb{Z}_{45}$ ,  $\mathbb{Z}_9 \times \mathbb{Z}_5$ , or  $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ . None of these contain a subgroup of order 10, as the order of a subgroup must divide the order of the group.

Statement 2 is true. By the definition of a normal subgroup, a subgroup  $H$  of a group  $G$  is normal if and only if for all  $g$  in  $G$ , the left coset  $gH$  is equal to the right coset  $Hg$ . This is equivalent to the condition that the number of left cosets of  $H$  is equal to the number of right cosets of  $H$ .

So the final answer is  $\boxed{\text{D. 'False, True'}}$ .

\*\*\*\*\*

Answer Option 9:

Statement 1 is false. By the fundamental theorem of finite abelian groups, the only abelian groups of order 45 are isomorphic to either  $Z_{45}$  or  $Z_9 \times Z_5$ . Neither of these has a subgroup of order 10 (because 10 is not a divisor of 45).

Statement 2 is true. A subgroup  $H$  of a group  $G$  is normal if and only if it is invariant under conjugation by elements of  $G$ . This is equivalent to saying that the number of left cosets of  $H$  in  $G$  is equal to the number of right cosets of  $H$  in  $G$  (because conjugation by an element of  $G$  permutes the cosets of  $H$ ).

So the final answer is D. 'False, True'

\*\*\*\*\*

Question 44:

'Statement 1 | Every integral domain with characteristic 0 is infinite. Statement 2 | Every integral domain with prime characteristic is finite.', A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1 is true. An integral domain with characteristic 0 contains an isomorphic copy of the integers, and hence is infinite.

Statement 2 is false. Consider the ring of polynomials over a finite field. This is an integral domain and it has prime characteristic, but it is infinite.

So, the answer is C. 'True, False'.

=====

Answer Option 2:

Statement 1 is true. An integral domain with characteristic 0 contains an isomorphic copy of the integers, which is infinite.

Statement 2 is false. An integral domain with prime characteristic  $p$  is isomorphic to a subset of the polynomial ring with coefficients in  $\mathbb{Z}/p\mathbb{Z}$ , which is infinite.

So, the correct answer is C. 'True, False'.

=====

Answer Option 3:

Statement 1: True. An integral domain with characteristic 0 contains a copy of the integers (since  $1, 1+1, 1+1+1$ , etc. are all distinct), which implies that it must be infinite.

Statement 2: False. Any finite field is an integral domain, and there exist finite fields of any prime order (these fields have prime characteristic), but there also exist infinite fields (and hence infinite integral domains) of any prime characteristic.

So, the correct answer is C. 'True, False'.

=====

Answer Option 4:

Statement 1 | Every integral domain with characteristic 0 is infinite. This statement is True. The characteristic of an integral domain is the number of times one must add the multiplicative identity (1) to itself to reach the additive identity (0). If the characteristic is 0, this implies that this process can be repeated indefinitely, thus the domain is infinite.

Statement 2 | Every integral domain with prime characteristic is finite. This statement is False. For example, the field of integers modulo a prime number has prime characteristic and is finite, but the ring of polynomials over the integers modulo a prime number also has prime characteristic and is infinite.

Final Answer: C

=====

Answer Option 5:

Statement 1 is true. An integral domain with characteristic 0 contains a copy of the integers, and so it is infinite.

Statement 2 is false. The integers modulo  $p$ , where  $p$  is a prime, is an integral domain of prime characteristic  $p$ . However, the polynomial ring with coefficients in a field of prime order  $p$  is another example of an integral domain of characteristic  $p$ , and this ring is infinite.

So, the correct answer is C. 'True, False'.

=====

Answer Option 6:

Statement 1 | Every integral domain with characteristic 0 is infinite. This statement is true. An integral domain with characteristic 0 contains a copy of the integers within it, thus making it an infinite set.

Statement 2 | Every integral domain with prime characteristic is finite. This statement is false. Take for instance the polynomial ring  $(\mathbb{Z}/p\mathbb{Z})[x]$ , where  $p$  is prime. This is an integral domain with prime characteristic  $p$  and is clearly infinite.

So, the final answer is C. 'True, False'

=====

Answer Option 7:

Statement 1 is true, because in an integral domain with characteristic 0, the additive identity is 0 and the multiplicative identity is 1, and for any element  $a$  in the domain,  $a$  can be repeatedly added together to form an infinite set of elements within the domain.

Statement 2 is false, because in an integral domain with prime characteristic  $p$ , the sum of  $p$  copies of 1 results in 0 (the additive identity). However, if we consider the set that includes all multiples of 1 (which forms a set that is isomorphic to the integers mod  $p$ ), there are also other elements in the domain that are not in this set, making it an infinite domain.

So, the correct answer is C. 'True, False'.

=====

Answer Option 8:

Statement 1 is true. An integral domain with characteristic 0 means that no positive integer multiples of 1 (the multiplicative identity) adds up to 0. This implies the domain is infinite, because you can keep getting new elements by adding 1 to itself without ever cycling back to a previously obtained element.

Statement 2 is false. An integral domain with prime characteristic  $p$  means that  $p$  times 1 adds up to 0. However, this doesn't mean the domain is finite; for example, the field of integers mod  $p$  ( $\mathbb{Z}/p\mathbb{Z}$ , a common example of an integral domain with prime characteristic) is finite, but the ring of polynomials over a finite field (another example) is infinite.

So, the correct answer is: C. 'True, False'.

=====

Answer Option 9:

A characteristic of an integral domain refers to the number of times you have to add the multiplicative identity (1) to itself to get the additive identity (0). If this never happens, the characteristic is zero. If it does happen, the number of times required is the characteristic, which must be a prime number.

Statement 1 is True: An integral domain with characteristic 0 means you can keep adding 1 to itself indefinitely without returning to 0. Thus, it is infinite.

Statement 2 is False: An integral domain with prime characteristic  $p$  means you return to 0 after adding 1 to itself  $p$  times. However, this doesn't mean the domain is finite. For example, the integers mod  $p$  forms an infinite integral domain of characteristic  $p$  as you can keep adding 1 to itself  $p$  times to get a cycle but the elements (equivalence classes) themselves are infinite.

So, the final answer is C. 'True, False'

\*\*\*\*\*

Question 45:

'Let A and B be sets,  $f: A \rightarrow B$  and  $g: B \rightarrow A$  be functions such that for all  $a \in A$ ,  $g(f(a)) = a$ . Statement 1 | The function  $f$  must necessarily be injective. Statement 2 | The function  $f$  must necessarily be surjective.', A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1: True. If there exists distinct elements  $a_1$  and  $a_2$  in A such that  $f(a_1) = f(a_2)$ , then  $g(f(a_1)) = g(f(a_2)) = a_1$  according to the given condition. This contradicts the assumption that  $a_1$  and  $a_2$  are distinct. Therefore,  $f$  must be injective.

Statement 2: False. Nothing is given about the relationship between  $g$  and  $f$ , so  $f$  doesn't necessarily have to be surjective.

So, the final answer is C. 'True, False'

\*\*\*\*\*

Answer Option 2:

Statement 1: True - The function  $f$  must be injective. If it were not, then two different elements of A, say  $a_1$  and  $a_2$ , would be mapped to the same element in B. But then  $g$  would map this element back to both  $a_1$  and  $a_2$ , which is impossible.

Statement 2: False - The function  $f$  need not be surjective. There could be elements in B which are not mapped to by any element in A via  $f$ .  $g$  could still map these elements to any element in A.

So the final answer is: C. 'True, False'

\*\*\*\*\*

Answer Option 3:

Statement 1: True. If  $f$  is not injective, then there exist distinct elements  $a_1, a_2$  in A such that  $f(a_1) = f(a_2)$ . But then,  $g(f(a_1)) = g(f(a_2))$  which implies  $a_1 = a_2$ , a contradiction.

Statement 2: False. Even though  $g(f(a)) = a$  for all  $a$  in A, it doesn't mean that  $f$  is surjective. It is possible that there are elements in B which are not mapped by any element in A.

So, the final answer is C. 'True, False'.

\*\*\*\*\*

Answer Option 4:

Statement 1 is true. If  $f$  is not injective, there exist  $a_1, a_2$  in A such that  $a_1 \neq a_2$  and  $f(a_1) = f(a_2)$ . Applying  $g$  to both sides of  $f(a_1) = f(a_2)$  will give  $g(f(a_1)) = g(f(a_2))$  which implies  $a_1 = a_2$ , contradicting  $a_1 \neq a_2$ .

Therefore,  $f$  must be injective.

Statement 2 is false. The condition  $g(f(a)) = a$  for all  $a$  in A does not require that every element in B is mapped to by  $f$ . Therefore,  $f$  does not have to be surjective.

Therefore, the final answer is C. 'True, False'.

\*\*\*\*\*

Answer Option 5:

The function  $g(f(a)) = a$  implies that for every  $a$  in A, there exists a unique  $f(a)$  in B, and for every  $f(a)$ , there exists a unique  $g(f(a))$  in A. This means  $f$  must be injective - there cannot be two different elements in A that map to the same element in B. Otherwise,  $g$  would not be well-defined (one value in B would map back to two different values in A).

However, there is no requirement that  $f$  must be surjective. It's not required that every  $b$  in B is the image of some  $a$  in A, because  $g$  is not necessarily defined for every element in B.

So, Statement 1 is true and Statement 2 is false. This gives us the final answer as C. 'True, False'.

\*\*\*\*\*

Answer Option 6:

Statement 1 is True: The function  $f$  must necessarily be injective. If  $f$  were not injective, it would mean there exist some  $a_1$  and  $a_2$  in A such that  $a_1 \neq a_2$  and  $f(a_1) = f(a_2)$ . This would imply that  $g(f(a_1)) = g(f(a_2))$ , which contradicts the given that  $g(f(a)) = a$  for all  $a$  in A.

Statement 2 is False: The function  $f$  doesn't need to be surjective. The fact that  $g(f(a)) = a$  for all  $a$  in A doesn't imply that for every  $b$  in B, there exists an  $a$  in A such that  $f(a) = b$ .

So the correct answer is C. 'True, False'.

\*\*\*\*\*

Answer Option 7:

Statement 1 | True: If  $f$  were not injective, then there exist some  $a_1, a_2$  in A such that  $a_1 \neq a_2$  and  $f(a_1) = f(a_2)$ . Then,  $g(f(a_1)) = g(f(a_2))$ , or  $a_1 = a_2$ , a contradiction.

Statement 2 | False: It is not necessary for  $f$  to be surjective. For instance, consider the function  $f: \mathbb{R} \rightarrow \mathbb{R}$  defined as  $f(x) = x^2$ , and  $g: \mathbb{R} \rightarrow \mathbb{R}$  defined as  $g(y) = \sqrt{y}$  if  $y \geq 0$ , and  $g(y) = -\sqrt{-y}$  if  $y < 0$ . Then,  $g(f(x)) = x$  for all  $x$  in  $\mathbb{R}$ . However,  $f$  is not surjective as there do not exist any  $x$  in  $\mathbb{R}$  such that  $f(x) = -1$ .

So, the final answer is C. 'True, False'

\*\*\*\*\*

Answer Option 8:

Statement 1: True. If  $f$  is not injective, then there exist  $a_1$  and  $a_2$  in A such that  $a_1 \neq a_2$  and  $f(a_1) = f(a_2)$ . But then  $g(f(a_1)) = g(f(a_2))$ , so  $a_1 = a_2$ , which is a contradiction.

Statement 2: False.  $f$  does not necessarily have to be surjective. Consider  $A = B = \{1, 2, 3\}$  with  $f(x) = g(x) = 1$  for all  $x$  in A. We see that  $f$  is not surjective, as  $f(x) \neq 2$  or  $3$  for any  $x$  in A, but  $g(f(a)) = a$  for all  $a$  in A.

So, the final answer is C. 'True, False'.

\*\*\*\*\*

Answer Option 9:

Firstly, let's consider the statement 1. The function  $f$  is injective if for every  $a$  and  $b$  in  $A$ , if  $f(a) = f(b)$  then  $a = b$ . Given that  $g(f(a)) = a$  for all  $a$  in  $A$ , if we suppose  $f(a) = f(b)$ , then applying  $g$  to both sides of the equation gives  $g(f(a)) = g(f(b))$ , or  $a = b$ . So, the function  $f$  must necessarily be injective.

Next, let's consider the statement 2. The function  $f$  is surjective if for every  $b$  in  $B$ , there is an  $a$  in  $A$  such that  $f(a) = b$ . However, it doesn't necessarily have to be true. Let's consider an example where  $A = \{1, 2\}$  and  $B = \{3, 4, 5\}$ , with  $f(a) = a + 2$  and  $g(b) = b - 2$ . For all  $a$  in  $A$ ,  $g(f(a)) = a$  holds. However,  $f$  is not surjective because there is no  $a$  in  $A$  such that  $f(a) = 5$ .

So, the final answer is 'True, False', or C.

\*\*\*\*\*

Question 46:

'Statement 1 | For any two groups  $G$  and  $G'$ , there exists a homomorphism of  $G$  into  $G'$ . Statement 2 | Every homomorphism is a one-to-one map.', A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1 | False: A homomorphism is a map between two groups that preserves the group operations. However, not every pair of groups has a homomorphism between them.

Statement 2 | False: A homomorphism is not necessarily a one-to-one map. It is possible for different elements in the domain to map to the same element in the codomain.

Final Answer: B. 'False, False'

\*\*\*\*\*

Answer Option 2:

Statement 1 is true. We can always define a homomorphism of  $G$  into  $G'$  by mapping every element of  $G$  to the identity element of  $G'$ . However, Statement 2 is false. Not all homomorphisms are one-to-one.

For example, the homomorphism we defined in Statement 1 is not one-to-one unless  $G$  consists of a single element. So, the correct answer is C. 'True, False'.

\*\*\*\*\*

Answer Option 3:

Homomorphism is a map between two groups that preserves the group operation. However, not all pairs of groups have a homomorphism from one to the other, so Statement 1 is False. Also, homomorphisms are not necessarily one-to-one. Consider, for example, the homomorphism from the integers to the integers mod 2 under addition, which maps both 2 and 4 to 0. So Statement 2 is also False. Therefore, the correct answer is B. 'False, False'.

\*\*\*\*\*

Answer Option 4:

Statement 1 is true. For any two groups  $G$  and  $G'$ , there exists a trivial homomorphism of  $G$  into  $G'$ . The trivial homomorphism sends all elements of  $G$  to the identity element of  $G'$ .

Statement 2 is false. Not every homomorphism is a one-to-one map. For example, the trivial homomorphism mentioned above is not one-to-one unless  $G$  is a group consisting of a single element.

Final Answer: C. 'True, False'

\*\*\*\*\*

Answer Option 5:

Statement 1: False. There does not exist a group homomorphism from any nontrivial group to the trivial group  $\{0\}$ .

Statement 2: False. Homomorphisms are not necessarily injective (one-to-one). For example, consider the homomorphism from the group of integers under addition to the group of integers modulo 2 under addition. This map is not one-to-one because, for example, it maps both 2 and -2 to 0.

So, both statements are false. The answer is B. 'False, False'.

\*\*\*\*\*

Answer Option 6:

'Statement 1' is true. The constant map sending each element of  $G$  to the identity element of  $G'$  is a homomorphism of  $G$  into  $G'$ . 'Statement 2' is false. Not every homomorphism is a one-to-one map. For example, consider the homomorphism from the additive group of integers to the additive group of integers modulo 2 that sends each integer to its remainder when divided by 2. This is not one-to-one since, for instance, it sends both 2 and 4 to the same element. So, final answer: C.

\*\*\*\*\*

Answer Option 7:

Statement 1 is true. We can always map every element of  $G$  to the identity of  $G'$ , which is a valid (though possibly not very interesting) homomorphism.

Statement 2 is false. Not all homomorphisms are one-to-one. As an example, consider the homomorphism from the integers under addition to the integers modulo 2 under addition, which maps every even integer to 0 and every odd integer to 1. This is not one-to-one since, for example, 2 and 4 are distinct but map to the same image.

So the correct answer is C: 'True, False'.

\*\*\*\*\*

Answer Option 8:

Statement 1 is true. There always exists the zero map, which sends every element of  $G$  to the identity of  $G'$ .

However, statement 2 is false. Not all homomorphisms are one-to-one. For example, consider the homomorphism from the group of integers under addition to the group of integers modulo 2 under addition, which sends each integer to its remainder when divided by 2. This is not one-to-one since, for example, 2 and 4 are sent to the same place.

So, the correct answer is C: 'True, False'.

\*\*\*\*\*

Answer Option 9:

Statement 1: False. It is not necessarily the case that for any two arbitrary groups  $G$  and  $G'$ , there exists a homomorphism of  $G$  into  $G'$ . For example, consider the group  $G=\{1\}$  under multiplication and the group  $G'=\{0\}$  under addition. There is no homomorphism from  $G$  to  $G'$  because 1 in  $G$  cannot be mapped to any element in  $G'$  while preserving the group operation.

Statement 2: False. Not all homomorphisms are one-to-one (injective). Consider the homomorphism from the group of integers under addition to the group of integers modulo 2 under addition. This homomorphism maps every even integer to 0 and every odd integer to 1. Clearly, this is not a one-to-one map.

So, both statements are False. Final answer: B.

\*\*\*\*\*





Question 47:

'Statement 1 | A homomorphism may have an empty kernel. Statement 2 | It is not possible to have a nontrivial homomorphism of some finite group into some infinite group.', A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1: A homomorphism may indeed have an empty kernel. For example, the identity function on non-identity elements of a group is a homomorphism with an empty kernel. So, the first statement is true.

Statement 2: It is indeed possible to have a nontrivial homomorphism of some finite group into some infinite group. For example, consider the group of integers under addition and the cyclic group of order 2.

The map that takes even integers to the identity and odd integers to the other element is a nontrivial homomorphism. So, the second statement is false.

So, the final answer is C. 'True, False'.

\*\*\*\*\*

Answer Option 2:

Statement 1 is False: A homomorphism always has a kernel, although the kernel may only contain the identity element. It can never be empty.

Statement 2 is False: Homomorphisms from finite groups into infinite groups can indeed exist, and they can be nontrivial. For example, consider the map from the group of integers modulo 2 to the group of integers under addition that sends 1 to 2.

So, the correct answer is B. 'False, False'.

\*\*\*\*\*

Answer Option 3:

Statement 1: A homomorphism may have an empty kernel. This is False. The kernel of a group homomorphism is always a subgroup of the original group, and every group has at least the trivial subgroup. So a homomorphism cannot have an empty kernel.

Statement 2: It is not possible to have a nontrivial homomorphism of some finite group into some infinite group. This is False. As an example, consider the homomorphism from the integers modulo 2 to the integers defined by 1 maps to 1 and 0 maps to 0. This is a nontrivial homomorphism from a finite group to an infinite group.

So, the final answer is B. 'False, False'

\*\*\*\*\*

Answer Option 4:

Statement 1: The kernel of a group homomorphism is the set of elements in the domain that map to the identity in the codomain. The identity of the domain always maps to the identity of the codomain.

Therefore, a homomorphism cannot have an empty kernel. This statement is False.

Statement 2: It is indeed possible to have a nontrivial homomorphism of a finite group into an infinite group. For instance, consider the group homomorphism from the integers mod 2 into the integers given by mapping 0 to 0 and 1 to 1. This is a nontrivial homomorphism of a finite group into an infinite group. This statement is False.

Final answer: B. 'False, False'

\*\*\*\*\*

Answer Option 5:

Statement 1: A homomorphism may have an empty kernel. - False. The kernel of a group homomorphism is always a subgroup of the domain, and therefore must contain at least the identity element of that group. It can never be empty.

Statement 2: It is not possible to have a nontrivial homomorphism of some finite group into some infinite group. - False. It is possible to have a nontrivial homomorphism from a finite group to an infinite group.

For instance, consider the homomorphism from the integers modulo  $n$  to the integers under addition, defined by mapping each integer  $x$  modulo  $n$  to  $nx$  in the integers. This is nontrivial if  $n > 1$ .

So, the correct answer is B. 'False, False'

\*\*\*\*\*

Answer Option 6:

Statement 1 | A homomorphism may have an empty kernel.

This statement is false. The kernel of a homomorphism is never empty because it always contains the identity element of the original group. The identity element is always mapped to the identity element in the target group.

Statement 2 | It is not possible to have a nontrivial homomorphism of some finite group into some infinite group.

This statement is also false. For example, consider the group  $\mathbb{Z}$  (the integers with addition) and the cyclic group  $\mathbb{Z}/n\mathbb{Z}$  of order  $n$ . The map  $f: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}$  defined by  $f([a]) = a$  is a group homomorphism. This is a nontrivial homomorphism from a finite group to an infinite group.

Final Answer: B. 'False, False'

\*\*\*\*\*

Answer Option 7:

Statement 1: A homomorphism may have an empty kernel.

This statement is FALSE. The kernel of a group homomorphism is always a subgroup of the domain, and every group has at least the trivial subgroup  $\{e\}$ , where  $e$  is the identity element. So, a homomorphism cannot have an empty kernel.

Statement 2: It is not possible to have a nontrivial homomorphism of some finite group into some infinite group.

This statement is FALSE. For example, the group of integers under addition, denoted by  $\mathbb{Z}$ , is an infinite group. The cyclic group of order  $n$ , denoted by  $C_n$ , is a finite group. If  $n > 1$ , there is a nontrivial homomorphism from  $C_n$  to  $\mathbb{Z}$ , given by  $f(x) = nx$ .

So, the correct answer is (B) 'False, False'.

\*\*\*\*\*

Answer Option 8:

Statement 1: A homomorphism may have an empty kernel. This statement is False. The kernel of a group homomorphism is always a subgroup of the domain, and the smallest subgroup of any group is the trivial group, not the empty set.

Statement 2: It is not possible to have a nontrivial homomorphism of some finite group into some infinite group. This statement is False. For example, consider the group of integers under addition, which is infinite, and the cyclic group of order 2. The homomorphism that sends 0 to 0 and 1 to 2 is nontrivial.

Therefore, the correct answer is B. 'False, False'

\*\*\*\*\*

Answer Option 9:

Statement 1 is true. The kernel of a group homomorphism is the set of elements in the domain that map to the identity in the codomain. If a homomorphism maps no elements of the domain to the identity of the codomain (besides the identity of the domain itself), then it has an empty kernel.

Statement 2 is false. We can have a nontrivial homomorphism from a finite group to an infinite group. For example, consider a homomorphism from the group  $\mathbb{Z}_2$  (the integers modulo 2) to the group of integers under addition. We can define this homomorphism to map 0 to any even number, and 1 to any odd number.

So the final answer is C. 'True, False'.

\*\*\*\*\*

Question 48:

'Find all  $c$  in  $\mathbb{Z}_3$  such that  $\mathbb{Z}_3[x]/(x^3 + x^2 + c)$  is a field.', A. '0', B. '2', C. '1', D. '3'

=====

Answer Option 1:

For the polynomial ring  $\mathbb{Z}_3[x]/(x^3 + x^2 + c)$  to be a field, the polynomial  $x^3 + x^2 + c$  must be irreducible over  $\mathbb{Z}_3$ . This means it must have no roots in  $\mathbb{Z}_3$ .

We can check that  $x = 0, 1, 2$  are not roots of the polynomial if and only if  $c = 2$ .

So, the answer is  $\boxed{2}$ . Final Answer: B

=====

Answer Option 2:

The polynomial  $x^3 + x^2 + c$  has a root in  $\mathbb{Z}_3$  if and only if the quotient ring is not a field. So,  $x^3 + x^2 + c$  must not have a root in  $\mathbb{Z}_3$ .

We see that  $x^3 + x^2 + 2$  takes on all the values in  $\mathbb{Z}_3$ . Therefore, the only possible value of  $c$  is  $\boxed{0}$ . Final answer: A

=====

Answer Option 3:

For  $\mathbb{Z}_3[x]/(x^3 + x^2 + c)$  to be a field, the polynomial  $x^3 + x^2 + c$  must be irreducible over  $\mathbb{Z}_3$ , which means that it has no roots in  $\mathbb{Z}_3$ . For  $c = 0, 1, 2$ , we find that the polynomial takes the values 1, 2, and 0, respectively, at  $x = 0$ , and takes the values 2, 2, and 0, respectively, at  $x = 1$ . Therefore, the polynomial has a root in  $\mathbb{Z}_3$  if and only if  $c \neq 1$ . Thus, the only value of  $c$  for which  $\mathbb{Z}_3[x]/(x^3 + x^2 + c)$  is a field is  $c = 1$ . The correct answer is C.

=====

Answer Option 4:

The polynomial  $x^3 + x^2 + c$  is cubic, so  $\mathbb{Z}_3[x]/(x^3 + x^2 + c)$  is a field if and only if  $x^3 + x^2 + c$  is irreducible over  $\mathbb{Z}_3$ . The polynomial  $x^3 + x^2 + c$  is irreducible if and only if it has no roots in  $\mathbb{Z}_3$ .

If  $c = 0$ , then  $x = 0$  is a root of  $x^3 + x^2 + c$ .

If  $c = 1$ , then  $x = 1$  is a root of  $x^3 + x^2 + c$ .

If  $c = 2$ , then  $x = 2$  is a root of  $x^3 + x^2 + c$ .

So the answer is  $\boxed{A}$ . Final answer: A

=====

Answer Option 5:

For  $\mathbb{Z}_3[x]/(x^3 + x^2 + c)$  to be a field, the polynomial  $x^3 + x^2 + c$  must be irreducible over  $\mathbb{Z}_3$ . If  $c = 0$ , the polynomial factorizes as  $x^2(x + 1)$ , so  $c \neq 0$ . If  $c = 1$ , the polynomial is  $x^3 + x^2 + 1$ . Testing the elements of  $\mathbb{Z}_3$ , we see that none of them are roots of this polynomial, so it's irreducible and  $\mathbb{Z}_3[x]/(x^3 + x^2 + 1)$  is a field. If  $c = 2$ , the polynomial is  $x^3 + x^2 + 2$ , which factorizes as  $(x + 1)^3$ , so  $c \neq 2$ . Therefore, the only value of  $c$  for which  $\mathbb{Z}_3[x]/(x^3 + x^2 + c)$  is a field is  $c = 1$ . Final Answer: C

=====

Answer Option 6:

In order for  $\mathbb{Z}_3[x]/(x^3 + x^2 + c)$  to be a field, the polynomial  $x^3 + x^2 + c$  should be irreducible, which means it must have no roots and must not be factorizable.

The roots of the polynomial  $x^3 + x^2 + c$  are solutions to the equation  $x^3 + x^2 + c = 0$ . Since we are working in  $\mathbb{Z}_3$ , we only need to check for  $x = 0, 1, 2$ .

When  $x = 0$ ,  $c = 0$  for the equation to hold. When  $x = 1$ , the equation becomes  $1 + 1 + c = 0 \pmod 3$ , which implies  $c = 1$ . When  $x = 2$ , the equation becomes  $8 + 4 + c = 0 \pmod 3$ , which simplifies to  $c = 1$ .

So, for  $x^3 + x^2 + c$  to be irreducible (and hence for  $\mathbb{Z}_3[x]/(x^3 + x^2 + c)$  to be a field),  $c$  must not be 0 or 1. This leaves us with  $c = \boxed{2}$ . Final Answer: B

=====

Answer Option 7:

For the quotient ring  $\mathbb{Z}_3[x]/(x^3 + x^2 + c)$  to be a field, the polynomial  $x^3 + x^2 + c$  must be irreducible over  $\mathbb{Z}_3$ . This means that it doesn't have a root in  $\mathbb{Z}_3$  (since if it did, that root would be a divisor of the polynomial).

A polynomial in  $\mathbb{Z}_3$  has a root of 0 if and only if the constant term is 0. The polynomial  $x^3 + x^2 + c$  has a root of 0 if and only if  $c = 0$ . Therefore  $c = 0$  is not a solution.

A polynomial in  $\mathbb{Z}_3$  has a root of 1 if and only if the sum of its coefficients is 0. The polynomial  $x^3 + x^2 + c$  has a root of 1 if and only if  $1 + 1 + c = 0$ . Which gives  $c = 1$  is not a solution.

A polynomial in  $\mathbb{Z}_3$  has a root of 2 if and only if the sum of its coefficients multiplied by 2, and then reduced mod 3, is 0. The polynomial  $x^3 + x^2 + c$  has a root of 2 if and only if  $2 + 2(2) + 2c = 0$ . Which gives  $c = 2$  is not a solution.

Therefore, the only solution is  $\boxed{3}$ . Final answer: D

=====

Answer Option 8:

The polynomial  $x^3 + x^2 + c$  is irreducible in  $\mathbb{Z}_3[x]$  if and only if it has no roots in  $\mathbb{Z}_3$ . These roots are 0, 1, and 2.

If  $c = 0$ , then

$x^3 + x^2 = x^2(x + 1) = 0$ , which has roots 0 and 1, so  $c$  cannot be 0.

If  $c = 1$ , then

$x^3 + x^2 + 1 = 0$  implies that  $x^3 = -x^2 - 1 = x^2 + 2$ . If  $x = 0$ , then  $x^3$  and  $x^2$  are both 0, so  $x = 0$  is not a root. If  $x = 1$ , then  $x^3 = 1$  and  $x^2 = 1$ , so  $x = 1$  is not a root. If  $x = 2$ , then  $x^3 = 2$  and  $x^2 = 1$ , so  $x = 2$  is not a root. Therefore,  $c = 1$  works.

If  $c = 2$ , then

$x^3 + x^2 + 2 = x^3 + x^2 - 1 = 0$ , which implies  $x^3 = -x^2 + 1 = x^2 + 1$ . If  $x = 0$ , then  $x^3$  and  $x^2$  are both 0, so  $x = 0$  is not a root. If  $x = 1$ , then  $x^3 = 1$  but  $x^2 = 1$ , so  $x = 1$  is a root.

Therefore,  $c = 2$  does not work.

Therefore, the possible values of  $c$  is  $\boxed{1}$ . Final answer: C

\*\*\*\*\*

Answer Option 9:

In order for  $\mathbb{Z}_3[x]/(x^3 + x^2 + c)$  to be a field, the polynomial  $x^3 + x^2 + c$  in  $\mathbb{Z}_3[x]$  must not have any roots in  $\mathbb{Z}_3$ . This is because if it does have a root, say  $a$ , then  $(x-a)$  divides  $x^3 + x^2 + c$ , which would imply that the quotient ring is not an integral domain, and thus not a field.

Since we are in  $\mathbb{Z}_3$ , we only need to check if 0, 1, or 2 are roots of the polynomial.

If  $c = 0$ , then the polynomial is  $x^3 + x^2$ , which is 0 when  $x = 0$  or  $x = 1$ .

If  $c = 1$ , then the polynomial is  $x^3 + x^2 + 1$ , which is 0 when  $x = 1$ .

If  $c = 2$ , then the polynomial is  $x^3 + x^2 + 2$ , which is 0 when  $x = 0$ .

But if  $c = 3$ , then the polynomial is  $x^3 + x^2 + 3$ , but in  $\mathbb{Z}_3$ , 3 is equivalent to 0, so it also has roots.

So, the only choice for  $c$  that makes  $\mathbb{Z}_3[x]/(x^3 + x^2 + c)$  a field is  $c = \boxed{2}$ . Final Answer: B

\*\*\*\*\*

Question 49:

'Statement 1 | If a R is an integral domain, then  $R[x]$  is an integral domain. Statement 2 | If R is a ring and  $f(x)$  and  $g(x)$  are in  $R[x]$ , then  $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$ .'; A. 'True, True', B. 'False, False', C. 'True, False', D. 'False, True'

=====

Answer Option 1:

Statement 1 is true. The polynomial ring over an integral domain is itself an integral domain.

Statement 2 is also true. The degree of the product of two polynomials is the sum of the degrees of the individual polynomials.

Hence, the final answer is A. 'True, True'.

=====

Answer Option 2:

Statement 1: An integral domain is a nonzero commutative ring in which the product of any two nonzero elements is nonzero. The polynomial ring  $R[x]$  also has this property if R is an integral domain.

Therefore, the statement is True.

Statement 2: This statement is true because the degree of the product of two polynomials is the sum of the degrees of the polynomials. Therefore, the statement is True.

Final Answer: A. 'True, True'

=====

Answer Option 3:

Statement 1: True. The ring of polynomials over an integral domain is an integral domain.

Statement 2: True. In a ring, the degree of the product of two polynomials is the sum of the degrees of the polynomials. This is because the degree of a product is determined by the highest power of  $x$  that appears, which is the sum of the highest powers in each factor.

Therefore, the answer is A. 'True, True'.

=====

Answer Option 4:

Statement 1 is true. An integral domain is a commutative ring which has no zero divisors besides zero itself. If the ring R is an integral domain, then the polynomial ring  $R[x]$  (the set of all polynomials with coefficients in R) is also an integral domain.

Statement 2 is also true. The degree of the product of two polynomials is the sum of their degrees, provided the two polynomials are not zero.

So, the correct answer is A. 'True, True'.

=====

Answer Option 5:

Statement 1: True. The ring of polynomials over an integral domain is also an integral domain. This is because multiplication of polynomials corresponds to convolution of their coefficients, thus if a product of two polynomials is zero then their coefficient sequences must both be eventually zero, which means at least one of the polynomials is the zero polynomial, hence the domain has no zero divisors.

Statement 2: True. In general, for a ring R,  $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$  holds. This is because the degree of a product of two polynomials is the sum of the degrees of the polynomials.

Final Answer: A. 'True, True'

=====

Answer Option 6:

Statement 1 is true. If R is an integral domain, then  $R[x]$ , the ring of polynomials with coefficients in R, is also an integral domain. This is because if R is an integral domain, then it has no zero divisors, and the same is true of  $R[x]$ .

Statement 2 is also true. In any ring R, the degree of the product of two polynomials  $f(x)$  and  $g(x)$  in  $R[x]$  is equal to the sum of the degrees of  $f(x)$  and  $g(x)$ , provided that neither  $f(x)$  nor  $g(x)$  are the zero polynomial.

So, the answer is A. 'True, True'.

=====

Answer Option 7:

Both statements are true, so the correct answer is A.

Explanation:

Statement 1: An integral domain is a commutative ring with identity in which the product of any two nonzero elements is nonzero. The ring of polynomials over an integral domain inherits these properties. For example, the product of any two nonzero polynomials is a nonzero polynomial, so  $R[x]$  is also an integral domain.

Statement 2: If  $f(x)$  and  $g(x)$  are polynomials in  $R[x]$ , the degree of their product is indeed the sum of their degrees, provided neither of the polynomials is the zero polynomial. Otherwise, the degree of the zero polynomial is undefined. So, this statement is also true.

Therefore, the final answer is A: 'True, True'.

=====

Answer Option 8:

Both statements are true.

Statement 1: If R is an integral domain, then  $R[x]$  is an integral domain. This means that if R is a commutative ring in which the product of any two non-zero elements is non-zero (that is, it has no zero divisors), then the ring of polynomials with coefficients in R also has this property.

Statement 2: If  $R$  is a ring and  $f(x)$  and  $g(x)$  are in  $R[x]$ , then  $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$ . This is a fundamental property of the degree of a polynomial: the degree of the product of two polynomials is the sum of their degrees.

So, the correct answer is 'True, True'. Final Answer: A.

\*\*\*\*\*

Answer Option 9:

An integral domain is a nonzero commutative ring in which the product of any two nonzero elements is always nonzero. The polynomial ring  $R[x]$  over a ring  $R$  is the set of all polynomials with coefficients in  $R$ .

The operation of addition and multiplication are defined in the usual way of adding and multiplying polynomials.

Statement 1: If  $R$  is an integral domain, then  $R[x]$  is an integral domain. This is True. If  $R$  is an integral domain, meaning the product of any two nonzero elements is never zero, then the polynomial ring  $R[x]$  over  $R$  is also an integral domain. The product of any two nonzero polynomials will be a nonzero polynomial, since none of the coefficients of the product polynomial will be zero due to  $R$  being an integral domain.

Statement 2: If  $R$  is a ring and  $f(x)$  and  $g(x)$  are in  $R[x]$ , then  $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$ . This is also True. The degree of a polynomial is the highest power of  $x$  that appears with a nonzero coefficient.

When two polynomials are multiplied, the degree of the product is the sum of the degrees of the factors, assuming that  $R$  is a ring that doesn't have zero divisors (which would allow the degree of the product to be less than the sum of the degrees of the factors).

So, the correct choice is A, 'True, True'.

\*\*\*\*\*

Question 50:

'Find the maximum possible order for some element of  $Z_8 \times Z_{10} \times Z_{24}$ .'; A. '8', B. '120', C. '240', D. '24'

=====

Answer Option 1:

The order of an element in a direct product of groups is the least common multiple of the orders of its components. The maximum order of an element in  $Z_n$  is  $n$ , so the maximum possible order of an element in  $Z_8 \times Z_{10} \times Z_{24}$  is the least common multiple of 8, 10, and 24, which is  $\boxed{120}$ . Final answer: B

\*\*\*\*\*

Answer Option 2:

The order of an element in a direct product of groups is the least common multiple of the orders of the elements in each group. The maximum order of an element in  $\mathbb{Z}_n$  is  $n$ , so we want the least common multiple of 8, 10, and 24, which is  $\boxed{120}$ . Final Answer: B.

\*\*\*\*\*

Answer Option 3:

The order of an element in the direct product of groups is the least common multiple of the orders of the elements in the individual groups. The maximum order of an element in  $Z_n$  is  $n$ . Therefore, the maximum order of an element in  $Z_8 \times Z_{10} \times Z_{24}$  is the least common multiple of 8, 10, and 24, which is  $\boxed{120}$ . Final answer: B

\*\*\*\*\*

Answer Option 4:

Recall that the order of an element in a direct product is the least common multiple of the orders of each of its components. The maximum possible order for an element in  $Z_n$  is  $n$ , so the maximum possible order in  $Z_8 \times Z_{10} \times Z_{24}$  is the least common multiple of 8, 10, and 24, which is  $\boxed{120}$ . So, the correct option is B.

\*\*\*\*\*

Answer Option 5:

The order of an element in a direct product of groups is the least common multiple of the orders of its components. In this case, the possible orders in  $Z_8$ ,  $Z_{10}$ , and  $Z_{24}$  are divisors of 8, 10, and 24, respectively. Therefore, the maximum possible order of an element in the direct product is the least common multiple of 8, 10, and 24 which is  $\boxed{120}$ . Final answer: B.

\*\*\*\*\*

Answer Option 6:

The order of an element in a direct product of groups is the least common multiple of the orders of its components. In  $\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24}$ , the maximum order in each component is 8, 10, and 24, respectively. Therefore, the maximum order of an element in the direct product is  $\text{lcm}(8,10,24)=\boxed{120}$ . Final Answer: B

\*\*\*\*\*

Answer Option 7:

The order of an element in a direct product of groups is the least common multiple of the orders of the individual components of the element. The maximum order of an element in  $\mathbb{Z}_n$  is  $n$ .

Thus, to maximize the order of an element in  $\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24}$ , we should take an element of order 8 in  $\mathbb{Z}_8$ , an element of order 10 in  $\mathbb{Z}_{10}$ , and an element of order 24 in  $\mathbb{Z}_{24}$ .

The least common multiple of 8, 10, and 24 is 240, so the maximum possible order of an element in  $\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24}$  is  $\boxed{240}$ . Final answer:

C

\*\*\*\*\*

Answer Option 8:

The order of an element  $(a,b,c)$  of  $\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24}$  is the least common multiple of the orders of  $a$ ,  $b$ , and  $c$ . The order of an element  $a$  in  $\mathbb{Z}_n$  is  $n/\gcd(a,n)$ . Thus, the highest possible order in  $\mathbb{Z}_n$  is  $n$ . So, the maximum possible order of an element in  $\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24}$  is

$\text{lcm}(8,10,24)=\boxed{120}$ . Final Answer: B

\*\*\*\*\*

Answer Option 9:

An element in the product group  $Z_8 \times Z_{10} \times Z_{24}$  is of the form  $(a,b,c)$  where  $0 \leq a < 8$ ,  $0 \leq b < 10$ , and  $0 \leq c < 24$ . The order of the element  $(a,b,c)$  is the smallest positive integer  $n$  such that  $n(a,b,c) = (0,0,0)$ . Because  $Z_n$  is a cyclic group,  $na = 0$  in  $Z_n$  if and only if  $n$  is a multiple of the order of  $a$  in  $Z_n$ . Therefore, the order of  $(a,b,c)$  is the least common multiple of the orders of  $a$ ,  $b$ , and  $c$  in  $Z_8$ ,  $Z_{10}$ , and  $Z_{24}$ , respectively.

The order of an element  $a$  in a cyclic group of order  $n$  divides  $n$ , so the order of  $a$  in  $Z_8$  divides 8, the order of  $b$  in  $Z_{10}$  divides 10, and the order of  $c$  in  $Z_{24}$  divides 24. The least common multiple of divisors of 8, 10, and 24 is  $\text{lcm}(8,10,24) = 120$ . If  $a=4$ ,  $b=5$ , and  $c=12$ , then  $(a,b,c)$  has order 120 in  $Z_8 \times Z_{10} \times Z_{24}$ . Therefore, the maximum possible order of an element in  $Z_8 \times Z_{10} \times Z_{24}$  is  $\boxed{120}$ . Final Answer: B

\*\*\*\*\*