

Course outline

How does an NPTEL online course work?

Propositional Logic

Predicate Logic, Proof Strategies and Induction

Sets and Relations

Equivalence Relations, Partitions, Partial Orderings and Functions

Theory of Countability

Combinatorics Part I

Combinatorics Part II

Graph Theory Part I

Graph Theory Part II

Number theory

Abstract Algebra : Part I

Abstract Algebra : Part II

 Rings, Fields and Polynomials

 Polynomials Over Fields and Properties

 Finite Fields and Properties I

 Finite Fields and Properties II

 Primitive Element of a Finite Field

 Applications of Finite Fields

 Goodbye and Farewell

 Quiz : Week 12 Assignment

Video download

Live Session

Text transcripts

Week 12 Assignment

The due date for submitting this assignment has passed.

Due on 2021-04-14, 23:59 IST.

As per our records you have not submitted this assignment.

Rings, fields, polynomials over rings, polynomials over fields, polynomial factorization, finite fields, Characteristic, order and primitive element(s) of a finite field

1) Select the correct option(s) :

1 point

- There are no divisors of element 0 in a field
- Every ring is a field, but every field is not a ring
- $(\mathbb{R}-0,+,\cdot)$ is an example of a field
- None of the option are correct

No, the answer is incorrect.
Score: 0

Accepted Answers:
There are no divisors of element 0 in a field

 2) Which of the following is the GCD (greatest common divisor) of the following polynomials over \mathbb{F} , the field of rational numbers: $a^6 + a^3 + a + 1$ and a^{2^2+1} .

1 point

- a-1
- a+1
- a^2+1
- None of the given options

No, the answer is incorrect.
Score: 0

Accepted Answers:
 a^2+1

3) Which of the following is/are true?

1 point

- A degree d polynomial over fields will always have d roots
- A monic polynomial of degree d is a polynomial in x is one in which the coefficient of the highest power x is equal to unity
- If $f(x)$ is a polynomial and if $f(3)=0$, then 3 is a root of $f(x)$
- An irreducible polynomial over a field cannot be factored as a product of two non-constant polynomials

No, the answer is incorrect.
Score: 0

Accepted Answers:
A degree d polynomial over fields will always have d roots
A monic polynomial of degree d is a polynomial in x is one in which the coefficient of the highest power x is equal to unity
If $f(x)$ is a polynomial and if $f(3)=0$, then 3 is a root of $f(x)$
An irreducible polynomial over a field cannot be factored as a product of two non-constant polynomials

 4) The order and characteristic of the finite field \mathbb{F}_{2^8} are respectively:

1 point

- (256, 2)
- (2, 256)
- (256, 256)
- None of the answers are correct

No, the answer is incorrect.
Score: 0

Accepted Answers:
(256, 2)

5) Which of the following is/are true?

1 point

- In Shamir's (n,t) secret-sharing scheme, the scheme is secure even if t number of shares are available
- If a group is of prime order, then it is cyclic
- The multiplicative cyclic group \mathbb{Z}_p^* where p is prime, has p generators
- None of the answers are correct

No, the answer is incorrect.
Score: 0

Accepted Answers:
In Shamir's (n,t) secret-sharing scheme, the scheme is secure even if t number of shares are available
If a group is of prime order, then it is cyclic

 6) Let $R = \{ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a,b,c,d \in \mathbb{S} \}$. Choose the correct option(s).

1 point

- R is a ring under addition and multiplication when $\mathbb{S} = \mathbb{Q}$
- R is a ring under addition and multiplication when $\mathbb{S} = \mathbb{R}$ but not when $\mathbb{S} = \mathbb{Q}$
- R is not a ring under addition and multiplication for any $\mathbb{S} \subset \mathbb{R}$
- None of the given options

No, the answer is incorrect.
Score: 0

Accepted Answers:
 R is a ring under addition and multiplication when $\mathbb{S} = \mathbb{Q}$

 7) Let p be a prime. Choose the correct option(s):

1 point

- There are p^2 monic irreducible quadratics in $\mathbb{Z}_p[x]$
- There are $\frac{p(p-1)}{2}$ monic irreducible quadratics in $\mathbb{Z}_p[x]$
- There are $\frac{p(p^2+p-1)}{3}$ monic irreducible cubics in $\mathbb{Z}_p[x]$
- There are $\frac{p(p^2-1)}{3}$ monic irreducible cubics in $\mathbb{Z}_p[x]$

No, the answer is incorrect.
Score: 0

Accepted Answers:
There are $\frac{p(p-1)}{2}$ monic irreducible quadratics in $\mathbb{Z}_p[x]$
There are $\frac{p(p^2-1)}{3}$ monic irreducible cubics in $\mathbb{Z}_p[x]$

 8) Alice and $n-1$ of her remaining friends each have a (n,t) -Shamir share. Alice wishes to reconstruct the secret and asks her friends to send her their secret shares. However, s friends send Alice incorrect values in an attempt to stop her from learning the secret. Note that Alice does not know which shares are incorrect. Choose the correct option(s).

1 point

- Alice can detect that some shares are incorrect when $n = 10, t = 8$ and $s = 1$
- It is impossible for Alice to detect that some shares are incorrect when $n = 10, t = 8$ and $s = 1$
- Alice can detect that some shares are incorrect when $n = 10, t = 9$ and $s = 1$
- It is impossible for Alice to detect that some shares are incorrect when $n = 10, t = 9$ and $s = 1$

No, the answer is incorrect.
Score: 0

Accepted Answers:
Alice can detect that some shares are incorrect when $n = 10, t = 8$ and $s = 1$
It is impossible for Alice to detect that some shares are incorrect when $n = 10, t = 9$ and $s = 1$

 9) Suppose that the election committee of a college consists of three students and three professors. The result of election is encrypted using key k . The key k is shared between the six members. It is decided that the following combinations only can unlock the result:

1 point

- (I) all the three students together, OR
- (II) Any two professors together

 Choose the correct statement(s) about the secret-sharing for the key k ?

- Fixing the shares of students indeed fix the shares of professors
- Each party end up having a pair of shares at the end of secret sharing
- Either replicated secret sharing or Shamir's secret sharing techniques can be used to secret share the key k
- None of the given options

No, the answer is incorrect.
Score: 0

Accepted Answers:
Either replicated secret sharing or Shamir's secret sharing techniques can be used to secret share the key k

 10) Consider the following statements about a group G ?

1 point

- (I) G must be abelian if $(ab)^2 = a^2b^2, \forall a, b \in G$
- (II) G is abelian if $x = x^{-1}, \forall x \in G$

 Which of the following is true about the group G ?

- Only Option I is true
- Only Option II is true
- Both options I and II are true
- Both options I and II are false

No, the answer is incorrect.
Score: 0

Accepted Answers:
Both options I and II are true