Discrete Structures

Third Short Test

17–November–2020

---

1. Consider the set $\mathbb{Z}$ of all integers with the following operations, where s and t are constant integers.

$$a \oplus b = a + b + s,$$
$$a \odot b = a + b + tab.$$

Which of the following is a necessary and sufficient condition for $(\mathbb{Z}, \oplus, \odot)$ to be a ring?

(A) $s = t = -1$.
(B) $st = 1$.
(C) s and t can have any values.
(D) s and t can have any values with $t \neq 0$.

Solution Closure and associativity of $\oplus$ and $\odot$, and the existence of additive identity and additive inverse follow for any s, t. Associativity holds if and only if $st = 1$.

2. Consider the integral domain $\mathbb{Z}[\sqrt{7}] = \{a + b\sqrt{7} \mid a, b \in \mathbb{Z}\}$. Which of the following is **not** a unit in $\mathbb{Z}[\sqrt{7}]$?

(A) -1 **(B)** $-8 - 3\sqrt{7}$ **(C)** $37 - 14\sqrt{7}$ **(D)** $-127 + 48\sqrt{7}$

3. Let R be a ring with identity (or unity). An element $a \in R$ is called *idempotent* if $a^2 = a$. Which of the following statements is true? (Here $M_2(\mathbb{Z})$ denotes the set of all 2×2 matrices with integer entries.)

(A) R may contain a non-zero element which is both idempotent and nilpotent.
(B) If $R = M_2(\mathbb{Z})$, then the only idempotent elements of R are the zero matrix and the identity matrix.
(C) If R is not an integral domain, then R must contain an idempotent element other than 0 and 1.
(D) If R is not an integral domain, then R may contain an idempotent element other than 0 and 1.

4. Which of the following functions $f : \mathbb{Z} \to \mathbb{Z}$ is a homomorphism of the ring $(\mathbb{Z}, +, \cdot)$ to itself?

(A) $f(a) = 1$ **(B)** $f(a) = a$ **(C)** $f(a) = 2a$ **(D)** $f(a) = a^2$

5. If $f : K \to L$ is a homomorphism of fields with $f(1_K) = 1_L$, which of the following statements is **false**?

(A) f must be surjective.
(B) f must be injective.
(C) $f(a^{-1}) = f(a)^{-1}$ for all $a \in K$, $a \neq 0_K$.
(D) $f(a) = 0_L$ if and only if $a = 0_K$.

6. What is the inverse of an element a in the group $G = \{a \in \mathbb{R} \mid a > 0\}$ under the operation $\odot$ defined by $a \odot b = a^{\ln b}$?

(A) $1/e^a$ **(B)** $1/a$ **(C)** $1/\ln a$ **(D)** $e^{1/\ln a}$

Solution The identity element x is computed from: $a^{\ln x} = a \Rightarrow x = e$. Inverse of a is computed as: $a^{\ln a^{-1}} = e \Rightarrow \ln a^{-1} \ln a = \ln e = 1 \Rightarrow a^{-1} = e^{1/\ln a}$.

7. Let p be an odd prime. How many $x \in \mathbb{Z}_p^*$ satisfy $x \equiv x^{-1} \pmod{p}$?

(A) 1 **(B)** 2 **(C)** $(p-1)/2$ **(D)** $p - 1$

Solution Since p is a prime, $\mathbb{Z}_p$ is a field, and so a non-trivial polynomial congruence $f(x) \equiv 0 \pmod{p}$ can have at most $\deg(f)$ roots. Now, $x \equiv x^{-1} \pmod{p}$ is equivalent to $x^2 - 1 \equiv 0 \pmod{p}$, that is, $(x-1)(x+1) \equiv 0 \pmod{p}$, that is, $x \equiv \pm 1 \pmod{p}$. Since p is odd, $1 \not\equiv -1 \pmod{p}$.

8. Let G be a cyclic group with 135 elements. What is the size/order of the largest proper cyclic subgroup of G?

Solution 45 (Let g be a generator of G. Then, the order of g^3 is $\frac{135}{\gcd(3,135)} = \frac{135}{3} = 45$.)

9. If G is a cyclic group of order 72, how many distinct generators does G have?

Solution 24 (Euler totient function: $\phi(72) = 72 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) = 24$.)

10. Let $G = S_4$ (the symmetry group on four symbols), and let H be the subgroup

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \right\}.$$

How many left cosets of H are there in G?

Solution 6 (Since $|G| = 4! = 24$ and $|H| = 4$, there are $24/4 = 6$ left cosets of H in G.)