NBHM 2025 Solutions- Abstract Algebra

January 26, 2025

Solution 4:

Problem Statement: The prime elements of the ring $\mathbb{Z}[i]$, i.e., $a + bi$, $a, b \in \mathbb{Z}$, are called *Gaussian primes*. Which of the following are Gaussian primes?

Note. It suffices to state just the letter corresponding to a statement. If more than one statement is true, then all such must be identified.

(a) $5 + 0i$

(b) $0 + 7i$

(c) $3 + 5i$

(d) $4 + 5i$

Solution: Do by yourself using norm!
Answer: (b), (d)

Solution 6:

Problem Statement: Let S_{11} be the symmetric group on 11 letters. How many subgroups of order 11 are there in S_{11}?

Solution: We want to determine the number of subgroups of order 11 in S_{11}. Subgroups of order 11 are cyclic, and every element in such a subgroup has order 11 except for the identity.

The symmetric group S_{11} contains 11! elements. To form a subgroup of order 11, we focus on the 11-cycles, as these elements have order 11.

The total number of permutations forming an 11-cycle is given by:

$$\frac{11!}{11} = 10!.$$

Each cyclic subgroup of order 11 contains exactly 10 non-identity elements. Since each subgroup is formed by these 10 elements and the identity, we divide by 10 to avoid overcounting:

$$\frac{10!}{10} = 9!.$$

Hence, the total number of subgroups of order 11 in S_{11} is 9!.

Solution 7:

Problem Statement: For $n \geq 1$, let S_n denote the set of all permutations of $\{1, 2, \ldots, n\}$. Let p_n denote the probability of the event that a randomly chosen permutation does not fix any integer in its original position. Find

$$\lim_{n\to\infty} p_n.$$

Solution: `https://en.wikipedia.org/wiki/Derangement#Growth_of_number_of_derangements_as_n_approaches_%E2%88%9E`

Solution 15:

Problem Statement: What is the number of homomorphisms from the symmetric group S_7 to the alternating group A_8 (i.e., the subgroup of all even permutations in the symmetric group S_8)?

Solution: We are asked to determine the number of homomorphisms from the symmetric group S_7 to the alternating group A_8. By the first isomorphism theorem, we examine the kernel of a potential homomorphism. The following cases are possible for the quotient $S_7/\ker(\phi)$:

1. S_7/A_7, 2. S_7/S_7, 3. $S_7/\{e\}$.

Let us analyze each case: - Case 2, S_7/S_7, corresponds to the trivial homomorphism, contributing exactly one homomorphism. - Case 3, $S_7/\{e\}$, suggests an injective homomorphism. However, since S_n can only be embedded into A_{n+2}, this case is not possible. - Therefore, the only valid case is S_7/A_7, where the kernel is A_7. The problem then reduces to finding the number of subgroups of order 2 in A_8, as these subgroups correspond to nontrivial homomorphisms.

Subgroups of order 2 in A_8 are generated by involutions, and there are two possible types of involutions: - Products of two disjoint 2-cycles, - Products of four disjoint 2-cycles.

Subcase 1: Products of two disjoint 2-cycles To calculate the number of products of two disjoint 2-cycles, we use the formula for partitioning a set of n elements into s pairs. Specifically, the number of ways to partition 4 elements into two disjoint 2-cycles is given by:

$$\frac{n!}{\prod_{i=1}^{s}(k_i! m_i^{k_i})} = \frac{8!}{2! \cdot 2^2 \cdot 4! \cdot 1^4} = \frac{40320}{2 \cdot 4 \cdot 24 \cdot 1} = 210.$$

Thus, the total number of products of two disjoint 2-cycles is 210.

Subcase 2: Products of four disjoint 2-cycles Now, we calculate the number of products of four disjoint 2-cycles. The number of ways to partition 8 elements into four disjoint pairs (to form a product of four disjoint 2-cycles) is:

$$\frac{8!}{4! \cdot 2^4} = \frac{40320}{24 \cdot 16} = 105.$$

Thus, the total number of subgroups of order 2 in A_8 is the sum of the two cases:

$$210 + 105 = 315.$$

Including the trivial homomorphism, the total number of homomorphisms from S_7 to A_8 is:

$$315 + 1 = 316.$$

Thus, the total number of homomorphisms from S_7 to A_8 is 316.

Solution 23:

Problem Statement: Let $i := \sqrt{-1}$ denote a square root of -1.

(a) All subrings of $\mathbb{Q}[i]$ are unique factorization domains. *True/False*

(b) All subrings of $\mathbb{Q}$ are exactly of the form $\mathbb{Z}\left[\frac{1}{n}\right]$ for some non-zero integer n. *True/False*

Solution: *(a)* False.
Let us see for example the number 26 in the ring $\mathbb{Z}[5i]$. We will show that there are two different irreducible factorizations of 26 in this ring.

1. **Factorization 1:** $26 = 13 \times 2$

   First, observe that 13 and 2 are irreducible elements in $\mathbb{Z}[5i]$. Since neither of them can be factored further into non-unit elements of $\mathbb{Z}[5i]$, we conclude that this is one valid factorization of 26.

2. **Factorization 2:** $26 = (1 + 5i)(1 - 5i)$

   Now, let's consider another factorization. We can calculate:

   $$(1 + 5i)(1 - 5i) = 1^2 - (5i)^2 = 1 - (-25) = 1 + 25 = 26.$$

   Thus, we have another factorization of 26 into the product of two elements, $1 + 5i$ and $1 - 5i$, which are irreducible in $\mathbb{Z}[5i]$.

Conclusion:
We have now shown two different irreducible factorizations of 26 in $\mathbb{Z}[5i]$:

$$26 = 13 \times 2 \quad \text{and} \quad 26 = (1 + 5i)(1 - 5i).$$

Since these factorizations involve different irreducible elements and are not associates, we conclude that $\mathbb{Z}[5i]$ does not satisfy the unique factorization property, i.e., it is not a unique factorization domain.

(b) False.

A subring of $\mathbb{Q}$ that is not of the form $\mathbb{Z}\left[\frac{1}{n}\right]$ is the ring of rational integers of the form $\frac{a}{p^k}$, where $a \in \mathbb{Z}$ and p is a fixed prime number. The subring is given by:

$$S = \left\{ \frac{a}{p^k} : a \in \mathbb{Z}, k \in \mathbb{N} \right\},$$

where p is a prime number, a is an integer, and k is a natural number.

This ring is different from $\mathbb{Z}\left[\frac{1}{n}\right]$ because it contains rationals where the denominator is restricted to powers of a single prime p, as opposed to being allowed to be any integer n. The ring is a subring of $\mathbb{Q}$ but does not have the form $\mathbb{Z}\left[\frac{1}{n}\right]$ for any integer n.

Solution 29:

Problem Statement: Let $R = \mathbb{Z}/n\mathbb{Z}$ be the commutative ring of integers modulo n, and consider the polynomials

$$p(x) = x^2 + x + 1 \quad \text{and} \quad q(x) = x^4 + 2x^3 + x^2 + 2025x + 2024$$

from $R[x]$. The number of integers n, where $n \geq 10$, such that $p(x)$ divides $q(x)$ in $R[x]$ is equal to

Solution: We are given the commutative ring $R = \mathbb{Z}/n\mathbb{Z}$ and two polynomials

$$p(x) = x^2 + x + 1 \quad \text{and} \quad q(x) = x^4 + 2x^3 + x^2 + 2025x + 2024 \in R[x],$$

and are tasked with finding the number of integers $n \geq 10$ such that $p(x)$ divides $q(x)$ in $R[x]$.

To determine when $p(x)$ divides $q(x)$, we first perform the division of $q(x)$ by $p(x)$. The goal is to express $q(x)$ as a product of $p(x)$ and some polynomial, plus a remainder. Performing the division, we get

$$q(x) = (x^2 + x + 1)(x^2 + x + 2024) - 2025x^2.$$

For $p(x) = x^2 + x + 1$ to divide $q(x)$, the remainder $-2025x^2$ must be zero in $\mathbb{Z}/n\mathbb{Z}$. This implies

$$2025x^2 \equiv 0 \pmod{n},$$

which holds for all x if and only if

$$2025 \equiv 0 \pmod{n}.$$

Thus, n must divide 2025.

Now, we compute the divisors of 2025. First, we factorize 2025:

$$2025 = 5^2 \times 3^4.$$

The divisors of 2025 are all numbers of the form $5^a \times 3^b$, where $0 \leq a \leq 2$ and $0 \leq b \leq 4$. These divisors are:

$$1, 3, 5, 9, 15, 25, 27, 45, 75, 81, 135, 225, 405, 675, 2025.$$

Next, we identify the divisors of 2025 that are greater than or equal to 10. These divisors are:

$$15, 25, 27, 45, 75, 81, 135, 225, 405, 675, 2025$$

Thus, there are 11 such divisors.

Therefore, the number of integers $n \geq 10$ such that $p(x)$ divides $q(x)$ is equal to the number of divisors of 2025 greater than or equal to 10, which is 11.

Solution 37:

Problem Statement: Let p be a fixed prime and $\mathbb{F}_p$ be the finite field with p elements.

(a) Suppose $L \supset K \supset \mathbb{F}_p$ are field extensions such that $\mathrm{Gal}(L/K) = \mathbb{Z}/m\mathbb{Z}$ and $\mathrm{Gal}(K/\mathbb{F}_p) = \mathbb{Z}/n\mathbb{Z}$. Then, $\mathrm{Gal}(L/\mathbb{F}_p) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. *True/False*

(b) There exist infinitely many Galois extensions of $\mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}$. *True/False*

Solution:

(a) Suppose $L \supset K \supset \mathbb{F}_p$ are field extensions such that $\mathrm{Gal}(L/K) = \mathbb{Z}/m\mathbb{Z}$ and $\mathrm{Gal}(K/\mathbb{F}_p) = \mathbb{Z}/n\mathbb{Z}$. Then, we are to check if $\mathrm{Gal}(L/\mathbb{F}_p) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Let $p = 2$, $K = \mathbb{F}_4$, and $L = \mathbb{F}_8$. The extension $K/\mathbb{F}_2$ has degree 2, so $\mathrm{Gal}(K/\mathbb{F}_2) = \mathbb{Z}/2\mathbb{Z}$, thus $n = 2$. The extension L/K also has degree 2, so $\mathrm{Gal}(L/K) = \mathbb{Z}/2\mathbb{Z}$, and hence $m = 2$. However, the total extension $L/\mathbb{F}_2$ has degree 3, so $\mathrm{Gal}(L/\mathbb{F}_2) \cong \mathbb{Z}/3\mathbb{Z}$. This is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and hence the statement is *False*.

(b) Let L/K be a Galois extension, and consider its Galois group $\mathrm{Gal}(L/K)$, endowed with the Krull topology. This topology arises from the inverse system of finite Galois subextensions M of L/K, with the open subgroups of $\mathrm{Gal}(L/K)$ corresponding to $\mathrm{Gal}(L/M)$ for each such M. The Krull topology ensures that $\mathrm{Gal}(L/K)$ is a profinite group, meaning it is compact, Hausdorff, and totally disconnected.

The group $\mathrm{Gal}(L/K)$ can be expressed as the inverse limit

$$\mathrm{Gal}(L/K) = \varprojlim_{M \subseteq L} \mathrm{Gal}(M/K),$$

where M runs over all finite Galois subextensions of L/K. Compactness in this topology is an essential property, and it implies that every open cover of $\mathrm{Gal}(L/K)$ has a finite subcover. Moreover, the group is totally disconnected, as the connected components reduce to singletons.

Consider $\mathbb{Z}$, the additive group of integers, under the Krull topology. For $\mathbb{Z}$ to qualify as a Galois group, it must satisfy the properties of a profinite group. However, $\mathbb{Z}$ fails to meet these criteria. It is not compact, as an open cover such as $\{\{n\} \mid n \in \mathbb{Z}\}$ in the discrete topology does not admit a finite subcover. Furthermore, $\mathbb{Z}$ is not an inverse limit of finite groups. While $\mathbb{Z}$ is totally disconnected in the discrete topology, this alone is insufficient for it to be profinite.

The profinite completion of $\mathbb{Z}$, denoted $\widehat{\mathbb{Z}}$, is compact and profinite. However, $\mathbb{Z} \neq \widehat{\mathbb{Z}}$, which further confirms that $\mathbb{Z}$ cannot arise as the Galois group of any Galois extension L/K.

Thus, there are no Galois extensions of $\mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}$, as such a group does not satisfy the necessary topological properties under the Krull topology. *False.*

Solution 40:

Problem Statement: Let $S^1 \subset \mathbb{C}$ denote the unit circle, which forms a group under the operation $e^{i\theta} \cdot e^{i\gamma} = e^{i(\theta+\gamma)}$ with identity element $1 \in \mathbb{C}$. Define $G := \{a + ib \in S^1 : a, b \in \mathbb{Q}\}$. Note that G itself forms a subgroup of S^1.

(a) The group G is isomorphic to $\mathbb{Q}/\mathbb{Z}$. *True/False*

(b) For a fixed prime p, the subset $H := \{(a, b) \in G : a = \frac{r}{p^s} \text{ for some } r, s \in \mathbb{Z}\}$ forms a subgroup of G. *True/False*

Solution:

(a) Let $S^1 \subseteq \mathbb{C}$ denote the unit circle, which forms a group under the operation $e^{i\theta} \cdot e^{i\gamma} = e^{i(\theta+\gamma)}$ with identity element $1 \in \mathbb{C}$. Define $G := \{a + ib \in S^1 : a, b \in \mathbb{Q}\}$. Note that G forms a subgroup of S^1.

We aim to determine whether G is isomorphic to $\mathbb{Q}/\mathbb{Z}$.

The group $\mathbb{Q}/\mathbb{Z}$ has the property that every element has finite order. Hence, if G contains an element of infinite order, G cannot be isomorphic to $\mathbb{Q}/\mathbb{Z}$.

Consider the element $\frac{3}{5} + \frac{4}{5}i \in G$. Its order depends on whether the angle $\theta = \arcsin\left(\frac{4}{5}\right)$ is a rational multiple of π. If θ is not a rational multiple of π, then $\frac{3}{5} + \frac{4}{5}i$ has infinite order.

By Niven's theorem, if θ is a rational multiple of π, then $\sin(\theta)$ must take one of the following values: $0, \pm\frac{1}{2}, \pm 1$. Here, $\sin(\theta) = \frac{4}{5}$, which does not belong to this set. Thus, $\theta = \arcsin\left(\frac{4}{5}\right)$ is not a rational multiple of π, and the element $\frac{3}{5} + \frac{4}{5}i$ has infinite order.

Since G contains an element of infinite order, while every element of $\mathbb{Q}/\mathbb{Z}$ has finite order, we conclude that G is not isomorphic to $\mathbb{Q}/\mathbb{Z}$. Hence, *False*.

(b) Let $x = \frac{r_1}{p^{s_1}} + ib_1$ and $y = \frac{r_2}{p^{s_2}} + ib_2$ be two elements of H, where $r_1, r_2 \in \mathbb{Z}$, $s_1, s_2 \in \mathbb{Z}$, and $b_1, b_2 \in \mathbb{Q}$. We need to show that $xy^{-1} \in H$.

Since $y \in S^1$, we know that $|y| = 1$. Therefore, the inverse of y is given by:

$$y^{-1} = \frac{r_2}{p^{s_2}} - ib_2.$$

Now, we compute xy^{-1}:

$$xy^{-1} = \left(\frac{r_1}{p^{s_1}} + ib_1\right) \cdot \left(\frac{r_2}{p^{s_2}} - ib_2\right).$$

Expanding this product:

$$xy^{-1} = \frac{r_1 r_2}{p^{s_1+s_2}} - i\frac{r_1 b_2}{p^{s_1}} + i\frac{r_2 b_1}{p^{s_2}} + b_1 b_2.$$

The real part of xy^{-1} is:

$$\mathrm{Re}(xy^{-1}) = \frac{r_1 r_2}{p^{s_1+s_2}} + b_1 b_2.$$

The imaginary part of xy^{-1} is:

$$\mathrm{Im}(xy^{-1}) = \frac{r_2 b_1}{p^{s_2}} - \frac{r_1 b_2}{p^{s_1}}.$$

Both the real and imaginary parts are rational numbers:

- The real part can be written as $\frac{r_1 r_2 + b_1 b_2 p^{s_1+s_2}}{p^{s_1+s_2}}$, which could be written as $\frac{R}{p^S}$
- The imaginary part is a difference of two rational numbers, so it is also rational.

Thus, xy^{-1} has the form $\frac{r}{p^s} + ib$, where $r \in \mathbb{Z}$, $s \in \mathbb{Z}$, and $b \in \mathbb{Q}$.

Since xy^{-1} has the required form $\frac{r}{p^s} + ib$, where $r \in \mathbb{Z}$, $s \in \mathbb{Z}$, and $b \in \mathbb{Q}$, we conclude that $xy^{-1} \in H$. Therefore, H is closed under the operation of taking products and inverses, and by the one-step subgroup test, H is a subgroup of G. So, *True*.

Corrections are welcome at- virat[dot]algebraicgeometry[at]gmail[dot]com