Захарчук Наталія, ТМП-32

Варіант-1.

№1. • Група - мн-на G з бінарною операцією $*$ такою, що:

1) $*$ - асоціативна

2) $\exists$ нейтральний ел-т. $e \in G$

3) Для кожного ел-та $a \in G$:
$\exists$ обернений $a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e$

• Таблиця з трьох елементів $\{e, a, b\}$

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

• Таблиця з 4-ох елементів $\{e, a, b, c\}$

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

та

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

№2.

№2. Характеристика кільця - p-ння вигляду:

$n \cdot a = n + \ldots + n = 0$, де $a \in R$ (довільне кільця), $n \in \mathbb{N}$ - мінімальне.

Якщо n не існує, то кільце має характеристику 0.

Теорема Ферма:

Нехай $a \in \mathbb{Z}$, p - просте число, що не ділить a, тоді:

$a^{p-1} \equiv 1 \pmod p$

Теорема Ейлера:

Якщо $a \in \mathbb{Z}$ - взаємнопросте з $n \in \mathbb{N}$, то:

$a^{\Phi(n)} \equiv 1 \pmod n$, де

$\Phi(n)$ - фі - функція Ейлера.

Доведення т. Ферма:

Вважаємо, що $a \in \mathbb{Z}_p$, $a \neq 1$.

$\{1, 2, \ldots, p-1\} \subset \mathbb{Z}_p$ - група порядку $p-1$ відносно множення за модулем p.

Оск. порядок елемента скінченної групи ділить порядок групи, то

порядок елемента $a \in \mathbb{Z}_p$ ділить $p-1$, отже $a^{p-1} = 1$ в $\mathbb{Z}_p$.

Доведення теореми Ейлера:

Нехай $1 \le a < n$, a - взаємопросте з n. Порядок групи G_n дорівнює $\varphi(n)$, тоді $a^{\varphi(n)} = 1$ в $\mathbb{Z}_n$, а отже $a^{\varphi(n)} \equiv 1 \pmod{n}$.

№3. Теорема Кронекера

Нехай F - поле, $f(x) \in F[x]$ - многочлен ненульового степеня. Тоді існує розширення E поля F та $\alpha \in E$, таке, що $f(\alpha) = 0$.

Доведення:

Якщо F - поле, тоді $f(x) \in F[x]$ може бути розкладений у добуток незвідних многочленів. Цей розклад - єдиний з точністю до порядку множників та мультиплікативної константи.

многочлен $P(x)$ - незвідний та входить у розклад $f(x)$ на незвідні множники.

Оскільки ідеал $\langle P(x)\rangle \in$ максимальним ідеалом в $F[x]$, то $F[x]/\langle P(x)\rangle$ - поле.

Ототожнимо F з деяким підполем поля $F[x]/\langle P(x)\rangle$ шляхом відображення $\varphi: F \to F[x]/\langle P(x)\rangle$, де: ~~$\varphi(a) = a + \langle P(x)\rangle, a \in F$~~

$\varphi(a)$ - ізоморфізм поля F та підполя $\{a + \langle P(x)\rangle : a \in F\}$, оск:

1) сюр'єктивність виконується
2) ін'єктивність виконується
3) $\varphi(ab) = \varphi(a)\varphi(b)$
   $\varphi(a+b) = \varphi(a) + \varphi(b)$

$\Rightarrow$

$\Rightarrow F[x]/\langle P(x)\rangle$ - розширення F. - E.

Покажемо, що $\exists \alpha \in E : P(\alpha) = 0$.

Нехай $\alpha = x + \langle P(x)\rangle$, $\varphi_\alpha : F[x] \to E$:

$\varphi_\alpha(a_0 + a_1 x + \dots + a_n x^n) = a_0 + a_1(x + \langle P(x)\rangle) + \dots + a_n(x + \langle P(x)\rangle)^n$, де $a_0, a_1, \dots, a_n \in F$.

Тоді:

$\varphi_\alpha(a_0 + a_1 x + \dots + a_n x^n) = a_0 + a_1 x + \dots + a_n \alpha^n + \langle P(x) \rangle =$

$= \langle P(x) \rangle.$

Отже, $\varphi_\alpha(P(x)) = 0$ в E, отже $P(\alpha) = 0$ в E.

Доведено.

№4. б) x^3+1 - незвідний над Z_{11}.

Оск. незвідність - відсутність коренів

$Z_{11} = \{0, 1, \alpha, \dots, 10\} = F$

$Z_{11} / \langle x^3+1 \rangle$ - розширення Z_{11}

$\alpha = x + \langle x^3+1 \rangle$

$\alpha^3 + 1 = (x + \langle x^3+1 \rangle)^3 + 1 = x^3 + \langle x^3+1 \rangle + 1 =$

$= \langle x^3+1 \rangle + x^3 + 1 = \langle x^3+1 \rangle = 0$

$\alpha \in$ нулем x^3+1 в розширенні $Z_{11} / \langle x^3+1 \rangle$

Отже, б - так

4) Поле має характеристику 0 => F містить підполе, ізоморфного $\mathbb{Z}$ (F містить підполе, що ізоморфне $\mathbb{Q}$)

Алгебраїчно замкнене поле не буває скінченним.
А у нескінченних полів характеристика 0 або нескінченна.

Отже, 4 - так.

2) Група A_3 - циклічна група
За наслідком з т. Лагранжа, якщо G - простого порядку, то G - циклічна група.

$|A_3| = \frac{|S_3|}{2} = \frac{3!}{2} = 3.$

Підгрупи групи A_3 мають порядки: 1, 3, 2 - циклічні.

2 - так.

5) $\mathbb{Q}$ є ідеалом в $\mathbb{Q}(\sqrt{2})$

Критерій:

$I \subset R$ є ідеалом, якщо:

1) $a - b \in I$ (I - адитивна підгрупа кільця R)

2) $r \cdot i \in I$ $\forall r \in R$
$i \in I$

Відп:

5 - так, оск ~~[illegible]~~.

1) $\forall n \in \mathbb{N} : \exists G_n : x^2 = e, \forall x \in G_n$.

Не правда, оск. розглянемо $n = 3$.

$G_3 : x^2 \neq e, \forall x \in G_3$.

Для порядку 3 існує лише одна група, де не виконується умова, що $x^2 = e$, оск тоді було б:

$\{e, a, b\} : \begin{cases} e \cdot e = e \\ a \cdot a = e \\ b \cdot b = e \end{cases} \Rightarrow e = a = b \Rightarrow$ порядок 1

1 - ні.

3) Мінімальний порядок скінченої некомутативної групи - 6.

6 - найменший порядок (некомутативної) неабелевої групи.

Оск. 1 - абелева.

2, 3, 5 - циклічні => абелеві

4 - нециклічна, але абелева: $\mathbb{Z}_2 \times \mathbb{Z}_2$

Отже, 6 - найменший порядок

3 - так

№5. p, q - прості числа, $r \in \mathbb{N}$.
Знайти число генераторів груп $\mathbb{Z}_{pq}$, $\mathbb{Z}_{p^r}$

Розв'язання.

① $\mathbb{Z}_{pq}$

Розглянемо 2 випадки:

1) $p \neq q$

Знайдемо всі числа, які менше за pq та ~~вза~~ взаємнопрості з pq.

Це числа, які не є кратними p та q. Для q таких чисел $p-1$, а для p: $q-1$.

Тоді число генераторів для $\mathbb{Z}_{pq}$ при $p \neq q$:

$$(pq-1)-(p-1)-(q-1) = pq-p-q+1 = (p-1)(q-1)$$

2) якщо $p = q$

знайдемо числа, менші за p^2, їх буде: $p(p-1)$

Тоді генераторів буде: $p(p-1)$.

(2) $\mathbb{Z}_{p^q}$

Знову, $\mathbb{Z}_{p^q}$ матиме стільки генераторів, скільки їх має p^q, що є взаємнопростими до p^q. Тобто, потрібно виключити всі множники p. Дільники p^q, які знаходяться в $\mathbb{Z}_{p^q}$: $1, p, p^2, \dots, p^{q-1}$. Таким чином для $x \in \mathbb{Z}_{p^q}$, якщо $НСД(p, x) \neq 1$, для $x \in \mathbb{Z}_{p^q}$, тоді $НСД(p, x) = p^s$, для якого $s \in \{1, 2, \dots, q\}$.

Отже, $p^s \mid x$, і тоді $x = kp^s$ для деякого k. Тобто, $x = (kp^{s-1})p$.

Маючи, що $k, p \in \mathbb{Z}$, то $kp^{s-1} \in \mathbb{Z}$.

Таким чином, $x \in$ множниками p, а тільки елементи, що не взаємнопрості до $p^q \in$ множниками p.

Найменший множник p: $0p = 0$, найбільший: $p^q - p = p(p^{q-1} - 1)$

Отже, множники p в $\mathbb{Z}_{p^q}$:

$0, p, 2p, \dots, (p^{q-1}-1)p$.

Тоді в нас $p^{q-1}-1+1=p^{q-1}$ множників p в $\mathbb{Z}_{pq}$.

Тоді генераторів буде $pq-p^{q-1}$.

Відповідь: для $\mathbb{Z}_{pq}$ або $(p-1)(q-1)$ або $p(p-1)$

Для $\mathbb{Z}_{p^q}$: p^q-p^{q-1}