Разбор задач домашнего задания по алгебре на 12.03 для группы БПИ209
3 модуль
Автор: vk.com/yourkumir

66.2 в) . Какие из следующих множеств матриц образуют поле относительно обычных матричных операций

$$M = \left\{ \begin{pmatrix} x & y \\ ny & x \end{pmatrix} : x, y \in \mathbb{Z}_p \right\}, \text{где } p = 2, 3, 5, 7$$

Проверим все свойства по порядку:
1.0) Замкнутость сложения на множестве:

$$\begin{pmatrix} a & b \\ nb & a \end{pmatrix} + \begin{pmatrix} c & d \\ nd & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ n(b+d) & a+c \end{pmatrix} \in M$$

1.1) Матричное сложение ассоциативно.
1.2) Существование нейтрального элемента:

$$\exists e_0 = \begin{pmatrix} 0 & 0 \\ n \cdot 0 & 0 \end{pmatrix} : \ \forall m \in M \ \ e_0 + m = m + e_0 = m$$

1.3) Существование обратного элемента:

$$\forall m = \begin{pmatrix} a & b \\ nb & a \end{pmatrix} \in M \ \ \exists -m = \begin{pmatrix} -a & -b \\ n \cdot (-b) & -a \end{pmatrix} : \ m + (-m) = (-m) + m = e_0$$

1.4) Матричное сложение коммутативно.
2.0) Замкнутость умножения на множестве:

$$\begin{pmatrix} a & b \\ nb & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ nd & c \end{pmatrix} = \begin{pmatrix} ac+nbd & ad+bc \\ n(ad+bc) & ac+nbd \end{pmatrix} \in M$$

2.1) Матричное умножение ассоциативно.
2.2) Существование нейтрального элемента:

$$\exists e_1 = \begin{pmatrix} 1 & 0 \\ n \cdot 0 & 1 \end{pmatrix} : \ \forall m \in M \ \ e_1 \cdot m = m \cdot e_1 = m$$

2.3) Существование обратного элемента: Тут необходимо найти обратную матрицу

$$\begin{pmatrix} a & b \\ nb & a \end{pmatrix}^{-1} = \frac{1}{x^2 - ny^2} \begin{pmatrix} a & -b \\ -nb & a \end{pmatrix}$$

Вспомним критерий существования обратной матрицы: матрица должна быть невырожденной, то есть $det = x^2 - ny^2 \neq 0$. Тогда найдём такие $n \in \mathbb{Z}_p$, при которых данное неравенство выполнено для всех x, y, которые одновременно не равны 0.

2.3.1) $p = 2$
Пусть $n = 0$, тогда существуют $x = 0, y = 1$, что $x^2 - ny^2 = 0^2 - 0 * 1^2 = 0$, что противоречит нашему неравенству.
Пусть $n = 1$, тогда существуют $x = 1, y = 1$, что $x^2 - ny^2 = 1^2 - 1 * 1^2 = 0$, что противоречит нашему неравенству.
Таким образом, при $p = 2$ таких n не существует.

2.3.2) $p = 3$
Для $n = 0, 1$ ситуация аналогичная предыдущему пункту.
Пусть $n = 2$, тогда

x	0	0	1	1	1	2	2	2
y	1	2	0	1	2	0	1	2
$x^2 - 2y^2$	1	1	1	2	2	1	2	2

Таким образом, для $p = 3$ нам подходит только $n = 2$.

2.3.3) $p = 5$
Перебирать $5^2 - 1 = 24$ значения для каждого n можно, но не нужно. Посмотрим на наше неравенство иначе:

$$x^2 - ny^2 \neq 0 \Leftrightarrow n \neq \frac{x^2}{y^2} \Leftrightarrow n \neq \left(\frac{x}{y}\right),$$

то есть n не является квадратом, а значит мы просто можем перебрать все квадраты:

0^2	1^2	2^2	3^2	4^2
0	1	4	4	1

Таким образом, для $p = 5$ нам подходят $n = 2, 3$.

2.3.4) $p = 7$
Перебирать $7^2 - 1 = 48$ значений для каждого n можно, но опять же не нужно, поэтому воспользуемся результатом предыдущего пункта и переберем все квадраты:

0^2	1^2	2^2	3^2	4^2	5^2	6^2
0	1	4	2	2	4	1

Таким образом, для $p = 7$ нам подходят $n = 3, 5, 6$.

2.4) Матричное сложение коммутативно.
3) Матричное сложение дистрибутивно относительно умножения:

$$(a + b)c = ac + bc,\ c(a + b) = ca + cb$$

Ответ: данное множество является полем при $n = 2$ и $p = 3$; $n = 2, 3$ и $p = 5$; $n = 3, 5, 6$ и $p = 7$

66.17 Существет ли бесконечное поле положительной характеристики?

Да, приведем пример. Возьмем конечное поле $\mathbb{F}_k$ характеристики k, тогда опишем поле рациональных функций (дроби из многочленов) над данным полем $\mathbb{F}_k(x) = \{r = \frac{p}{q} \mid p, q\ (q \neq 0)\ \in \mathbb{F}_k[x]\}$
Считается, что $\frac{p_1}{q_1} = \frac{p_2}{q_2}$, если $p_1q_2 = p_2q_1$. Отсюда следует приведение дробей к общему знаменателю, то есть $dpq = dpq \Rightarrow \frac{dp}{dq} = \frac{p}{q}$ так что дроби можно приводить к общему знаменателю и складывать $\frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1q_2 + p_2q_1}{q_1q_2}$. Умножение дробей задается довольно естественно $\frac{p_1}{q_1} * \frac{p_2}{q_2} = \frac{p_1p_2}{q_1q_2}$.
Вы можете проверить свойства данных операций, учитывая, что любой многочлен $p \in \mathbb{F}_k[x]$ $p = \frac{p}{1}$, и выясните, что множество рациональных функций является полем относительно этих операций.
Данное поле бесконечно и имеет характеристику $k > 0$.

64.2 а) Доказать, что кольцо $\mathbb{Z}[x]$ не является кольцом главных идеалов.

Докажем от противного. Пусть $\mathbb{Z}[x]$ - кольцо главных идеалов, тогда идеал $\langle 2, x\rangle$ тоже является главным, то есть $\exists f(x) \in \mathbb{Z}[x] : 2\mathbb{Z}[x] + x\mathbb{Z}[x] = f(x)\mathbb{Z}[x]$, тогда $2 \in \langle 2, x\rangle$ и $x \in \langle 2, x\rangle$ должны делиться на $f(x)$, но НОД$(2, x) = 1$, то есть $f(x) = \pm 1$, а значит идеал совпадает со всем кольцом.
Мы пришли к противоречию $\langle 2, x\rangle$ - многочлены вида $2\mathbb{Z}[x] + x\mathbb{Z}[x]$, они имеют четный свободный член, а $\mathbb{Z}[x]$ - это множество всех многочленов, поэтому $\langle 2, x\rangle \neq \mathbb{Z}[x]$

64.41 а), в) Доказать, что:

а) $F[x]/\langle x - \alpha\rangle \cong F$, где F - поле
Используем теорему о гомоморфизме колец:
$f : F[x] \to F \ f(p(x)) = p(\alpha)$ - гомоморфизм
$kerf = \{p(x) \mid p(\alpha) = 0\} = \langle x - \alpha\rangle$ - ядро гомоморфизма
$Imf = F$, так как $\forall c \in F \ \exists p = c : \ p(\alpha) = c$

в) $\mathbb{R}[x]/\langle x^2 + x + 1\rangle \cong \mathbb{C}$
Используем теорему о гомоморфизме колец:
$f : \mathbb{R}[x] \to \mathbb{C} \ f(p(x)) = p(-\frac{1}{2} + \frac{i\sqrt{3}}{2})$ - гомоморфизм
$kerf = \{p(x) \mid p(-\frac{1}{2} + \frac{i\sqrt{3}}{2}) = 0$ и $p(-\frac{1}{2} - \frac{i\sqrt{3}}{2}) = 0\} = \langle (x + \frac{1}{2} - \frac{i\sqrt{3}}{2})(x + \frac{1}{2} + \frac{i\sqrt{3}}{2})\rangle = \langle x^2 + x + 1\rangle$ - ядро гомоморфизма
$Imf = \mathbb{C}$, так как $\forall c \in \mathbb{C} \ \exists p : \ p(-\frac{1}{2} + \frac{i\sqrt{3}}{2}) = c$

1286 Являются ли линейным подпространством все векторы плоскости, каждый из которых лежит на одной из осей координат Ox, Oy?

$V = \{v \mid v \in Ox \cup v \in Oy\}$ не является линейным подпространством (подмножеством линейного пространства, являющимся линейным простанством относительно тех же операций), так как не замкнуто на сложении векторов (сложив вектор $v_1 \in Ox$ и $c_2 \in Oy$ мы можем не получить $v_1 + v_2 = v_3 \ \ v_3 \in Ox$ или $v_3 \in Oy$).

1287 Являются ли линейным подпространством все векторы плоскости, концы которых лежат на данной прямой (начало любого вектора совпадает с началом координат)?

Данное подмножество векторов является линейным подпространством только в том случае, если эта прямая совпадает с осями координат Ox, Oy, иначе не замкнуто на умножении на число.

1288 Являются ли линейным подпространством все векторы плоскости, начала и концы которых лежат на одной прямой?

Данное подмножество векторов является линейным подпространством, так как замкнуто на сложении и на умножении на число из поля.

дополнительно
а) Найдите обратный (по умножению) к элементу $x^2 - x - 1 + \langle f \rangle$ в факторкольце $\mathbb{Z}_3[x]/\langle f \rangle$,
где $f(x) = x^4 + x^3 - x - 1$.
б) Является ли это факторкольцо полем?

б) Фактор-кольцо $\mathbb{F}[x]/\langle f \rangle$ является полем тогда и только тогда, когда $f(x)$ неприводим над $\mathbb{F}$
$f(x) = x^4+x^3-x-1$ имеет над $\mathbb{Z}_3$ корень 1, то есть многочлен приводим $\to$ факторкольцо не является полем.

а) Пусть $g(x) = x^2 - x - 1$, тогда НОД$(f(x), g(x)) = 1 \Rightarrow \alpha(x)f(x) + \beta(x)g(x) = 1$ и $\beta(x)$ - обратный элемент к $g(x)$

	$f(x)$	$g(x)$	преобразования
$x^4 + x^3 - x - 1$	1	0	(1)
$x^2 - x - 1$	0	1	(2)
$x^4 - x^3 - x^2$	0	x^2	$(3) = x^2(2)$
$2x^3 + x^2 - x - 1$	1	$-x^2$	$(4) = (1) - (3)$
$2x^3 - 2x^2 - 2x$	0	$2x$	$(5) = 2x(2)$
$x - 1$	1	$-x^2 - 2x$	$(6) = (4) - (5)$
$x^2 - x$	x	$-x^3 - 2x^2$	$(7) = x(6)$
1	x	$2x^3 + x^2 + 2$	$(8) = (7) - (2)$

$\beta(x) = 2x^3 + x^2 + 2$

дополнительно
Найдите количество элементов поля из 8 элементов, из которых извлекается кубический корень.
Поле из восьми элементов: $\mathbb{Z}_2[x]/\langle x^3 + x^2 + 1 \rangle = \{0, 1, x, x+1, x^2, x^2+x, x^2+1, x^2+x+1\}$
$0^3 = 0$
$1^3 = 1$
$x^3 = x^2 + 1$
$(x+1)^3 = x$
$(x^2)^3 = x^2 + x$
$(x^2 + x)^3 = x^2 + x + 1$
$(x^2 + 1)^3 = x^2$
$(x^2 + x + 1)^3 = x + 1$
То есть из всех элементов извлекается кубический корень.