№64.1 б.

1) Пусть $f(x) \in I$

Тогда $\forall y(x) \in F[x] \begin{cases} f(x) \cdot y(x) \in I \\ y(x) \cdot f(x) \in I, \end{cases}$ то

есть $\langle f(x) \rangle \subseteq I$

2) Пусть $g(x) \neq f(x) \cdot h(x)$, то есть $g(x) \notin \langle f(x) \rangle$. Пусть $g(x) \in I$.

Тогда, аналогично п.1, $\langle g(x) \rangle \subseteq I$, то есть $\langle f(x), g(x) \rangle \subseteq I$.

По алгоритму Евклида, $\exists h(x), q(x) \in F[x]$:

$f(x) \cdot h(x) + g(x) \cdot q(x) = \text{НОД}(f(x), g(x))$

Если $\text{НОД}(f(x), g(x)) = f(x)$, то $g(x) = f(x) \cdot e(x)$ – противоречие

Если $\text{НОД}(f(x), g(x)) = g(x)$, то $f(x) = g(x) \cdot p(x)$, то есть $g(x) = f(x) \cdot p^{-1}(x)$ – противоречие.

$\Rightarrow \begin{cases} \text{НОД}(f(x), g(x)) \neq f(x) \\ \text{НОД}(f(x), g(x)) \neq g(x) \end{cases}$

Заметим, что $t(x) = f(x) \cdot h(x) + g(x) \cdot q(x)$:

$\begin{cases} t(x) \neq f(x) \cdot z(x) \\ t(x) \neq g(x) \cdot y(x) \end{cases} \Rightarrow \begin{cases} t(x) \notin \langle f(x) \rangle \\ t(x) \notin \langle g(x) \rangle \end{cases} \Rightarrow$

$\Rightarrow t(x) \notin \langle f(x), g(x) \rangle$

$\Rightarrow g(x) \notin I$

3) По п.1-2, $\begin{cases} \langle f(x) \rangle \subseteq I \\ \forall g(x) \notin \langle f(x) \rangle \quad g(x) \notin I \end{cases} \Rightarrow$

$\Rightarrow \langle f(x) \rangle = I$

Ответ: $\{ \langle f(x) \rangle \mid f(x) \in F[x] \}$

№64.2,5.

~~Пусть $I = \{ x \cdot f(x) \}$~~

Пусть $I = \{ x \cdot f(x,y) + y \cdot g(x,y) \mid \forall f, g \in F[x,y] \}$

1) Пусть $h_1 = x \cdot f_1(x,y) + y \cdot g_1(x,y) \in I$ и

$h_2 = x \cdot f_2(x,y) + y \cdot g_2(x,y) \in I$.

Тогда $h_1 - h_2 = x(f_1(x,y) - f_2(x,y)) + y(g_1(x,y) - g_2(x,y)) \in I$

$\Rightarrow I$ – подгруппа $F[x,y]$ по сложению.

Очевидно, что $I \neq F[x,y]$, т.к.

$\forall f(x,y), g(x,y) \in F[x,y]$

$\underbrace{x \cdot f(x,y) + y \cdot g(x,y)}_{\in I} \neq 0x + 0y + 1 \in F[x,y]$

2) Заметим, что $\forall r \in F[x,y]$

$r = x \cdot u(x,y) + y \cdot v(x,y) + f \cdot 1$

↑ некоторый элемент F.

Тогда $\forall r \in F[x,y], a \in I$

$r \cdot a = a \cdot r = (x \cdot u(x,y) + y \cdot v(x,y) + f \cdot 1) \cdot (x \cdot f(x,y) + y \cdot g(x,y))$

$= x^2 u(x,y) f(x,y) + xy(u(x,y) \cdot g(x,y) + f(x,y) v(x,y)) +$
$+ y^2 v(x,y) \cdot g(x,y) + x \cdot f \cdot f(x,y) + y \cdot f \cdot g(x,y) =$

$= x(x \cdot u(x,y) \cdot f(x,y) + y \cdot (u(x,y) \cdot g(x,y) + f(x,y) \cdot v(x,y)) + f \cdot f(x,y)) +$
$+ y \cdot (y \cdot v(x,y) \cdot g(x,y) + f \cdot g(x,y)) \in I \Rightarrow$

$\Rightarrow I$ — идеал.

3) Очевидно, что $I \neq \langle q(x) \rangle$, то есть I — не главный идеал:

- $x+y \in I,\ x \in I \Rightarrow$ Если $I = \langle q(x) \rangle$

То $\begin{cases} x+y = q(x)\cdot t(x) \\ x = q(x)\cdot p(x) \end{cases} \Rightarrow \begin{cases} q(x) \mid x \\ q(x) \mid x+y \end{cases} \Rightarrow$

$\Rightarrow q(x) \mid \text{НОД}(x, x+y) \Rightarrow q(x) \mid 1 \Rightarrow q(x) = 1$

Но $\langle 1 \rangle = F(x,y) \neq I \Rightarrow I \neq \langle q(x) \rangle$

№ 4.41 б.

$\mathbb{R}[x]/\langle x^2+x+1 \rangle \cong \mathbb{C}$

$\langle x^2+x+1 \rangle = \{ f(x) \mid f(x) = (x^2+x+1)g(x) \}$

- $x^2+x+1 = 0$

$D = 1-4 = -3 \Rightarrow x = \frac{-1 \pm \sqrt{-3}}{2} = \frac{-1 \pm i\sqrt{3}}{2}$

Рассмотрим $\varphi: \mathbb{R}[x] \to \mathbb{C}$

такую, что $\varphi(f(x)) = f\left(\frac{-1+i\sqrt{3}}{2}\right)$

1) $\forall f, g \in \mathbb{R}[x]$ $\varphi(f(x)+g(x)) =$

$= \varphi(y(x)) = y\left(\frac{-1+i\sqrt{3}}{2}\right) = (f+g)\left(\frac{-1+i\sqrt{3}}{2}\right) =$

Пусть $y = f+g$

$= f\left(\frac{-1+i\sqrt{3}}{2}\right) + g\left(\frac{-1+i\sqrt{3}}{2}\right) =$

$= \varphi(f(x)) + \varphi(g(x))$

2) $\forall f, g \in \mathbb{R}[x]$ $\varphi(f(x)\cdot g(x)) = \varphi(y(x))$ (=)

$y = f \cdot g$

(=) $g\left(\frac{-1+i\sqrt{3}}{2}\right) = (f\cdot g)\left(\frac{-1+i\sqrt{3}}{2}\right) = f\left(\frac{-1+i\sqrt{3}}{2}\right) \cdot$

$\cdot g\left(\frac{-1+i\sqrt{3}}{2}\right) =$

$= \varphi(f(x)) \cdot \varphi(g(x))$

$\Rightarrow \varphi$ – гомоморфизм колец.

Найдем $\ker\varphi$: $\ker\varphi = \left\{ f(x) \in \mathbb{R}[x] \,\middle|\, f\left(\frac{-1+i\sqrt{3}}{2}\right) = 0 \right\}$

Т.к. $f(x) \in \mathbb{R}[x]$ и $f\left(\frac{-1+i\sqrt{3}}{2}\right) = 0$, то

$f\left(\frac{-1-i\sqrt{3}}{2}\right)=0 \Rightarrow \left(x-\frac{-1+i\sqrt{3}}{2}\right)\left(x-\frac{-1-i\sqrt{3}}{2}\right) \mid f(x)$

$\Rightarrow (x^2+x+1) \mid f(x) \Rightarrow \ker f = \{ f(x) \in \mathbb{R}[x] \mid (x^2+x+1) \mid f(x) \}$

$\Rightarrow \ker f = \langle x^2+x+1 \rangle$

Найдём $\operatorname{Im} \varphi$.

1) $\forall f(x) \in \mathbb{R}[x] \quad f\left(\frac{-1+i\sqrt{3}}{2}\right) \in \mathbb{C} \Rightarrow \operatorname{Im}\varphi \subseteq \mathbb{C}$

2) $\forall a+bi \in \mathbb{C} \quad \exists f(x) = (a+bi)(a-bi) = (a^2+b^2) \in \mathbb{R}[x]:$
$\varphi(f(x)) = a+bi \Rightarrow \mathbb{C} \subseteq \operatorname{Im}\varphi$

$\Rightarrow \operatorname{Im}\varphi = \mathbb{C}$

По теореме о гомоморфизме колец для φ:

$\mathbb{R}[x]/\langle x^2+x+1 \rangle \cong \mathbb{C}$

2.Т.д.

№66.2.б.

$K = \left(\left\{ \begin{pmatrix} x & y \\ ny & x \end{pmatrix} \middle| \; x, y \in \mathbb{R} \right\}; + ; \cdot \right)$

1) Очевидно, что $(K, +)$ – абелева группа;

2) Умножение ассоциативно

$$\begin{pmatrix} x_1 & y_1 \\ ny_1 & x_1 \end{pmatrix} \begin{pmatrix} x_2 & y_2 \\ ny_2 & x_2 \end{pmatrix} = \begin{pmatrix} x_1x_2 + ny_1y_2 & x_1y_2 + y_1x_2 \\ ny_1x_2 + nx_1y_2 & ny_1y_2 + x_1x_2 \end{pmatrix} \in K \Rightarrow$$ умножение замкнуто

$\Rightarrow (K, \cdot)$ – полугруппа

3) Очевидно, что умножение дистрибутивно по сложению

$\Rightarrow K$ – кольцо.

4) 1. $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in K$

2. $$\begin{pmatrix} x_2 & y_2 \\ ny_2 & x_2 \end{pmatrix} \begin{pmatrix} x_1 & y_1 \\ ny_1 & x_1 \end{pmatrix} = \begin{pmatrix} x_1x_2 + ny_1y_2 & y_1x_2 + x_1y_2 \\ ny_2x_1 + ny_1x_2 & ny_1y_2 + x_1x_2 \end{pmatrix}$$

$\Rightarrow$ умножение коммутативно

3. Пусть $\begin{pmatrix} x_1 & y_1 \\ ny_1 & x_1 \end{pmatrix} \begin{pmatrix} x_2 & y_2 \\ ny_2 & x_2 \end{pmatrix} = O$

2) $\begin{cases} x_1x_2 + n y_1 y_2 = 0 \\ y_1x_2 + x_1y_2 = 0 \end{cases} \Rightarrow x_1 = \frac{-n y_1 y_2}{x_2}$

$\Rightarrow y_1x_2 - \frac{n y_1 y_2^2}{x_2} = 0$

$y_1 x_2^2 - n y_1 y_2^2 = 0$

$y_1(x_2 - y_2\sqrt{n})(x_2 + y_2\sqrt{n}) = 0$

- $y_1 = 0 \Rightarrow x_1 = 0 \Rightarrow \begin{pmatrix} x_1 & y_1 \\ n y_1 & x_1 \end{pmatrix} = 0 \Rightarrow$ не делитель 0.

$\Rightarrow x_2 = \pm y_2\sqrt{n} \Rightarrow$ делители нуля существуют при $\sqrt{n} \in \mathbb{R}$.

- Если $n < 0$, то делителей нуля нет $\Rightarrow$ K – целостное кольцо.

3) $\exists\, a = \begin{pmatrix} x & y \\ ny & x \end{pmatrix} \in K$

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

$= \begin{pmatrix} \frac{x}{x^2-ny^2} & \frac{-y}{x^2-ny^2} \\ n \cdot \frac{-y}{x^2-ny^2} & \frac{x}{x^2-ny^2} \end{pmatrix} \in K \Rightarrow$

$\Rightarrow \forall a \in K \ \exists a^{-1} \in K : a \cdot a^{-1} = 1 (=E)$

$\Rightarrow K$ — поле

Ответ: поле при $n < 0$

№66.2. б.

$$K = \left(\left\{ \begin{pmatrix} x & y \\ ny & x \end{pmatrix} \middle| x, y \in \mathbb{Z}_7 \right\}; +; \cdot \right)$$

1) Аналогично п.б., K — кольцо.

2) 1. $E \in K$

2. Аналогично б, умножение коммутативно

3. Делителей нуля нет тогда и только тогда, когда $\forall y_2 \ y_2\sqrt{n} \notin \mathbb{Z}_7$.

a) $n = 0 \Rightarrow x_2 = 1, y_2 = 0 : \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = 0$

b) $n = 1 \Rightarrow x_2 = y_2$

c) $n = 2 \Rightarrow x_2 = 3y_2$ ($3^2 = 2$)

d) $n = 3 \Rightarrow \forall a \in \mathbb{Z}_7 \ a^2 \neq n$

e) $n = 4 \Rightarrow x_2 = 2y_2$ ($2^2 = 4$)

f) $n=5 \Rightarrow \forall a \quad a^3 \neq n$

g) $n=6 \Rightarrow \forall a \quad a^3 \neq n$

$\Rightarrow K$ — целостное кольцо при $n=3,5,6$

3) Аналогично б очевидно, что

Если K — целостное кольцо, то K — поле.

Ответ: поле при $n=3,5,6$

№66.21.

$f(x)$; $\deg f(x) \leq 3$; $f(x) \in \mathbb{Z}_5[x]$;

x	0	1	2	4
$f(x)$	3	3	0	4

Пусть $f(x) = ax^3 + bx^2 + cx + d$

Тогда
$$\begin{cases} f(0) = d = 3 \\ f(1) = a+b+c+d = 3 \\ f(2) = 3a + 4b + 2c + d = 0 \\ f(4) = 4a + b + 4c + d = 4 \end{cases}$$

$$\begin{cases} d=3 \\ a+b+c=0 \\ a+2b+3=0 \\ 3a+3c=1 \end{cases} \qquad \begin{cases} d=3 \\ a+c=2 \\ b+2=0 \\ a+2b+3=0 \end{cases}$$

$$\begin{cases} d=3 \\ b=3 \\ a+c=2 \\ a+4=0 \end{cases} \qquad \begin{cases} a=1 \\ b=3 \\ c=1 \\ d=3 \end{cases}$$

$\Rightarrow f(x) = x^3+3x^2+x+3$

Ответ: ↗

№624в

$x^2+2x+3=0$ в F_{11}

~~$x^2+2x+4+1=0$~~ $x^2+2x+1+2=0$

~~$(x+2)^2+1=0$~~ $(x+1)^2+2=0$

~~$(x+2)^2=10$~~ $(x+1)^2=9$

~~$x+2=$~~ $\left[\begin{array}{l} x+1=3 \\ x+1=8 \end{array}\right. \quad \left\{\begin{array}{l} x=2 \\ x=7 \end{array}\right.$

$0^2=0 \quad 5^2=3$
$1^2=1 \quad 6^2=3$
$2^2=4 \quad 7^2=5$
$3^2=9 \quad 8^2=9$
$4^2=5 \quad 9^2=4 \quad 10^2=1$

Ответ: $x \in \{2,7\}$.

№68.58.

$f(x) = x^3 + 2x^2 + 4x + 1$ в $F_5[x]$

$x = 2 \Rightarrow f(x) = f(2) = 2^3 + 2 \cdot 2^2 + 4 \cdot 2 + 1 =$

$= 3 + 3 + 3 + 1 = 0$

$\Rightarrow f(x) : (x+3)$

$$\begin{array}{r|l} x^3+2x^2+4x+1 & x+3 \\ \hline -\,x^3+3x^2 & x^2+4x+2 \\ \hline 4x^2+4x & \\ -\,4x^2+2x & \\ \hline 2x+1 & \\ -\,2x+1 & \\ \hline 0 & \end{array}$$

$\Rightarrow f(x) = (x+2)(x^2+4x+2)$

x	x^2+4x+2
0	2
1	2
2	4
3	3
4	4

$\Rightarrow x^2+4x+2$ неприводим

$\Rightarrow f(x) = (x+2)(x^2+4x+2)$ неприводим.

№68.5 г.

г) $f(x) = x^4 + 3x^3 + 2x^2 + x + 4$ в $F_5[x]$

x	f(x)
0	4
1	1
2	4
3	2
4	3

$\Rightarrow f(x) = (x^2+ax+b)(x^2+cx+d) =$

$= x^4 + \underline{cx^3} + \underline{bx^2} + \underline{ax^3} + \underline{acx^2} + \underline{adx} + bx^2 + bcx + bd =$

$= x^4 + x^3(a+c) + x^2(d+ac+b) + x(ad+bc) + bd$

$\begin{cases} a+c=3 \Rightarrow \\ d+ac+b=2 \\ ad+bc=1 \\ bd=4 \Rightarrow \end{cases}$

$\begin{cases} a+c=3 \\ ac=2 \\ 4a+c=1 \end{cases} \Rightarrow \begin{cases} a=1 \\ c=2 \end{cases}$

$\begin{cases} b=1 \\ d=4 \end{cases}$ $\begin{cases} b=4 \\ d=1 \end{cases}$ симметричные случаи.

$\begin{cases} b=2 \\ d=2 \end{cases} \Rightarrow \begin{cases} 2(a+c)=1 \\ ac=3 \\ a+c=3 \end{cases} \Rightarrow a, c \notin F_5$

$\begin{cases} b=3 \\ d=3 \end{cases} \Rightarrow \begin{cases} a+c=3 \\ 3(a+c)=1 \\ ac=1 \end{cases} \Rightarrow a, c \notin F_5$

$\Rightarrow f(x) = (x^2+x+1)(x^2+2x+4)$

Ответ:

№1

Рассмотрим $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle \cong \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$

•	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

- $x^3+x+1 \sim 0$ (3-й неприводим) $x^4 = x(x^3) \sim x(x+1) = x^2+x$

  $x^3 \sim x+1$

  $x^3+x \sim 1$

№2.

1) $F_{11}[x]/_{\langle x^2+a\rangle}$ – поле, тогда и только тогда, когда x^2+a неприводим над F_{11}.

• Если x^2+a приводим, то

$\exists f, g \in F_{11}[x]: x^2+a = f\cdot g \Rightarrow$

$\Rightarrow \exists F, G \in F_{11}[x]/_{\langle x^2+a\rangle}: F = f + \langle x^2+a\rangle$

$G = g + \langle x^2+a\rangle \Rightarrow$

$\Rightarrow F\cdot G = fg + \langle x^2+a\rangle = x^2+a+\langle x^2+a\rangle =$

$= \langle x^2+a\rangle \Rightarrow$

$\Rightarrow$ существуют делители нуля.

x	x^2
0	0
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4

$10^2 = 1$

$\Rightarrow x^2+a$ неприводим при $a \in \{2, 6, 7, 8, 10\}$

2) $|U(K)| = |K| - 1 = 11^2 - 1 = 120$

3) Образующие элементы в $U(K)$ (примитивные) — взаимно-простые с $|U(K)|$, то есть их $\varphi(|U(K)|) = \varphi(120) = \varphi(2^3 \cdot 3 \cdot 5) =$

$= (2^3 - 2^2) \cdot 2 \cdot 4 = 4 \cdot 2 \cdot 4 = \boxed{32}$

Ответ: 1) a^q, $q \in \{3, 6, 7, 8, 10\}$

2) 120

3) 32