

Конечные кольца и поля — 1

1. Докажите, что $\mathbb{F}_5[x]/(x+2) \cong \mathbb{F}_5$.
2. Докажите, что $\mathbb{F}_3[x]/(x^2+2) \cong \mathbb{F}_3 \times \mathbb{F}_3$, опишите явно этот изоморфизм (для каждого элемента укажите, в какой он переходит).
3. Найдите такой многочлен $p(x) \in \mathbb{F}_3[x]$, что
а) $\mathbb{F}_3[x]/(p(x)) \cong \mathbb{Z}_3$, б) $\mathbb{F}_3[x]/(p(x)) \cong \mathbb{Z}_9$, в) $\mathbb{F}_3[x]/(p(x)) \cong \mathbb{Z}_2 \times \mathbb{Z}_3$
или докажите его отсутствие.
4. Пусть \mathbb{k} — поле, $(p(x))$ — идеал кольца $\mathbb{k}[x]$. Обозначим $\alpha = x + I$ — класс эквивалентности x . Покажите, что α является корнем многочлена $p(t)$ в кольце $\mathbb{k}[x]/(p(x))$.
5. Объясните следствие из предыдущей задачи: кольцо $\mathbb{k}[x]/(p(x))$ можно понимать как минимальное кольцо, содержащее \mathbb{k} и корень многочлена $p(x)$.
6. Для каждого многочлена второй степени в $p(x) \in \mathbb{F}_2[x]$ постройте кольцо $\mathbb{F}[\alpha]$, где α — корень многочлена $p(x)$. Укажите кольца, которые являются полями, найдите идемпотенты и идеалы в каждом полученном кольце. Укажите, какие кольца изоморфны $\mathbb{F}_2 \times \mathbb{F}_2$.
7. Докажите, что $\mathbb{F}_3[\alpha]$, где α — корень многочлена $x^2 + x + 2$, является полем. Найдите порядок по умножению $\alpha + 2$ в этом поле.

Решение. Покажем, что многочлен $p(x) = x^2 + x + 2$ неприводим над \mathbb{F}_3 . Так как этот многочлен степени не выше 3, достаточно проверить, что он не имеет в \mathbb{F}_3 корней. Проверяем:

$$p(0) = 2, \quad p(1) = 1, \quad p(2) = p(-1) = 2.$$

Многочлен $p(x)$ неприводим, а следовательно идеал $(x^2 + x + 2)$ максимален в $\mathbb{F}_3[x]$, поэтому $\mathbb{F}_3[\alpha] \cong \mathbb{F}_3[x]/(x^2 + x + 2)$ — поле.

Так как α корень $p(x)$, в поле $\mathbb{F}_3[\alpha]$ выполняется $\alpha^2 + \alpha + 2 = 0$, отсюда: $\alpha^2 = 2\alpha + 1$.

Найдем порядок элемента $\alpha + 2$. Мы знаем из теоремы Лагранжа, что порядок элемента — делитель порядка мультипликативной группы. Так как $\mathbb{F}_3[\alpha]$ поле, в котором 9 элементов:

$$0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2,$$

в мультипликативной группе 8 элементов (все, кроме 0). Поэтому $\text{ord}(\alpha + 2)$ может быть только 1, 2, 4, 8. Можно сообразить, что ответ будет лишь 4 или 8 (так как элементы порядка 1, 2 находятся в подполе \mathbb{F}_3), поэтому достаточно возвести $\alpha + 2$ в степень 4 и проверить, получим ли мы 1. Если нет, то ответ: 8. Возводим (не забываем, что арифметика по правилам \mathbb{F}_3):

$$(\alpha + 2)^2 = \alpha^2 + \alpha + 1 = (2\alpha + 1) + \alpha + 1 = 2$$

$$(\alpha + 2)^4 = 2^2 = 1$$

Таким образом $\text{ord}(\alpha + 2) = 4$.

8. Постройте поле из 4-х элементов и найдите порядок каждого элемента.

9. В поле $\mathbb{F}_3[\alpha]$, где α корень многочлена $x^2 + 1$, найдите порядок элемента α . Найдите элемент наибольшего порядка.

10. Найдите порядок элементов α и $2\alpha - 1$ в поле $\mathbb{F}_5[\alpha]$, где α корень многочлена $x^2 + 3x + 3$.

11. Найдите все неприводимые над полем \mathbb{F}_2 многочлены, степени не выше 4.

12. Найдите все неприводимые над полем \mathbb{F}_3 многочлены, степени не выше 2.

13. Постройте приводимый над \mathbb{F}_3 многочлен, не имеющий корней.

14. Определите количество неприводимых многочленов второй степени над \mathbb{F}_p , где: а) $p = 2$, б) $p = 3$, в) p — произвольное простое число.

15. В поле $\mathbb{F}_2[\alpha]$, где α — корень многочлена $p(x) = x^4 + x + 1$, найдите минимальный многочлен элемента $\alpha^3 + 1$ и все его корни.

16. Для кольца $\mathbb{K} = \mathbb{F}_5[\alpha]$, где α — корень многочлена $x^3 + 3x - 2$ выполните задания:

а) Докажите, что \mathbb{K} — поле.

б) Найдите порядок элемента $\alpha^2 + 2$ и его минимальный многочлен.

в) Найдите все корни многочлена $x^3 + 3x - 2$.

г) Найдите $(\alpha + 3)^{-1}$.

17. В поле $\mathbb{F}_3[\alpha]$, где α — корень многочлена $x^2 + 1$ решите уравнения:

а) $x + 2 = 0$ б) $x^2 + x + 1 = 0$ в) $x^2 + 1 = 0$ г) $x^2 + 2x + 2 = 0$