

Министерство образования и науки РФ
Уральский государственный экономический университет



Ю. Б. Мельников

Поле. Расширения полей

Раздел **электронного учебника**
для сопровождения практического занятия

Изд. 4-е, испр. и доп.



e-mail: melnikov@k66.ru,
melnikov@r66.ru

сайты:
<http://melnikov.k66.ru>,
<http://melnikov.web.ur.ru>

Екатеринбург
2012

Пример 1 поля порядка 4	5
Пример 2 к критерию алгебраичности элемента	29
Пример 3 расширения поля с помощью корня многочлена	52
Пример 4 расширения поля с помощью корня многочлена	169
Пример 5 к доказательству теоремы о расширении поля как фактор-кольце кольца многочленов	205
<i>Задание конечных полей таблицами Кели</i>	264

Задача I.1	265
<i>Нахождение расширения конечного поля с помощью корня полинома</i>	265
Задача II.2	266
Задача II.3	267
Задача II.4	268
Задача II.5	269
Задача II.6	270
<i>Нахождение многочлена, корнем которого является элемент расширения поля</i>	270

Задача III.7	271
Задача III.8	272
<i>Нахождение расширения поля как фактор-кольца кольца многочленов по некоторому идеалу</i>	272
Задача IV.9	273
Ответы и решения	274

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение.

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0				
1				
2				
3				

$x * y$	0	1	2	3
0				
1				
2				
3				

Так как 0 — нейтральный элемент **аддитивной группы поля**...

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1			
2	2			
3	3			

$x * y$	0	1	2	3
0				
1				
2				
3				

Так как 0 — нейтральный элемент **аддитивной группы поля...**

По **теореме об умножении на ноль в поле...**

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1			
2	2			
3	3			

$x * y$	0	1	2	3
0	0	0	0	0
1	0			
2	0			
3	0			

Так как 0 — нейтральный элемент **аддитивной группы поля...**

По **теореме об умножении на ноль в поле...**

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1			
2	2			
3	3			

$x * y$	0	1	2	3
0	0	0	0	0
1	0			
2	0			
3	0			

1 — нейтральный элемент мультипликативной группы поля...

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1			
2	2			
3	3			

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

1 — нейтральный элемент мультипликативной группы поля...

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1			
2	2			
3	3			

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

По **следствию о порядке конечного поля** искомое поле имеет **характеристику 2**.

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0		
2	2		0	
3	3			0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

По **следствию о порядке конечного поля** искомое поле имеет **характеристику 2**.

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0		
2	2		0	
3	3			0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

Положим $1 + 2 = 3$.

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	
2	2		0	
3	3			0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

Положим $1 + 2 = 3$.

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	
2	2	3	0	
3	3			0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

Положим $1 + 2 = 3$.

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	
2	2	3	0	
3	3			0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

Положим $1 + 2 = 3$.

Тогда $1 + 3 =$

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	
2	2	3	0	
3	3			0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

Положим $1 + 2 = 3$.

Тогда $1 + 3 = 1 + (1 + 2) =$

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	
2	2	3	0	
3	3			0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

Положим $1 + 2 = 3$.

Тогда $1 + 3 = (1 + 1) + 2 =$

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	
2	2	3	0	
3	3			0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

Положим $1 + 2 = 3$.

Тогда $1 + 3 = (1 + 1) + 2 = 2$.

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	
3	3	2		0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

Положим $1 + 2 = 3$.

Тогда $1 + 3 = (1 + 1) + 2 = 2$.

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	
3	3	2		0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

Тогда $2 + 3 =$

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	
3	3	2		0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

Тогда $2 + 3 = 2 + (1 + 2) =$

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	
3	3	2		0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

Тогда $2 + 3 = 2 + 1 + 2 = 1 + (2 + 2) =$

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	
3	3	2		0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

Тогда $2 + 3 = 2 + 1 + 2 = 1 + (2 + 2) = 1$.

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

Тогда $2 + 3 = 2 + 1 + 2 = 1 + (2 + 2) = 1$.

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

По теореме о цикличности мультипликативной группы поля Галуа...

Пример 1. Постройте поле порядка 4, т.е. поле с носителем из 4 элементов.

Решение. Пусть $GF(4) = \{0; 1; 2; 3\}$.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

По теореме о цикличности мультипликативной группы поля Галуа...

Вернуться к лекции?

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение.

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение. Имеем $2^2 = 2 * 2 =$

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение. Имеем $2^2 = 2 * 2 = 3 =$

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение. Имеем $2^2 = 2 * 2 = 3 = 1 + 2 =$

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение. Имеем $2^2 = 2 * 2 = 3 = 1 + 2 = 1 * 1 + 1 * 2$.

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение. Имеем $2^2 = 2 * 2 = 3 = 1 + 2 = 1 * 1 + 1 * 2$.

Значит, $2^2 + 1 * 2 + 1 * 1 = 0$.

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение. Имеем $2^2 = 2 * 2 = 3 = 1 + 2 = 1 * 1 + 1 * 2$.

Значит, $2^2 + 1 * 2 + 1 * 1 = 0$.

Таким образом, 2 является корнем многочлена $x^2 + x + 1$.

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение. Осталось проверить утверждение о **базисе**.

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение. Осталось проверить утверждение о **базисе**.

Воспользуемся **теоремой о линейных комбинациях базисных векторов**.

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение. **Линейная независимость** очевидна:

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение. **Линейная независимость** очевидна:

$$0 * 1 + 1 * 2 = 2 \neq 0,$$

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение. **Линейная независимость** очевидна:

$$0 * 1 + 1 * 2 = 2 \neq 0,$$

$$1 * 1 + 0 * 2 = 1 \neq 0,$$

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение. **Линейная независимость** очевидна:

$$0 * 1 + 1 * 2 = 2 \neq 0,$$

$$1 * 1 + 0 * 2 = 1 \neq 0,$$

$$1 * 1 + 1 * 2 = 3 \neq 0.$$

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение. **Линейная независимость** очевидна:

$$0 * 1 + 1 * 2 = 2 \neq 0,$$

$$1 * 1 + 0 * 2 = 1 \neq 0,$$

$$1 * 1 + 1 * 2 = 3 \neq 0.$$

Значит, $\alpha * 1 + \beta * 2 = 0$ только при $\alpha = \beta = 0$.

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение. Согласно **теореме о линейных комбинациях базисных векторов** осталось проверить, что $\{1; 2\}$ является **системой порождающих** для F .

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение.

$$0 = ? * 1 + ? * 2,$$

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение.

$$0 = 0 * 1 + 0 * 2,$$

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение.

$$0 = 0 * 1 + 0 * 2,$$

$$1 = ? * 1 + ? * 2,$$

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение.

$$0 = 0 * 1 + 0 * 2,$$

$$1 = 1 * 1 + 0 * 2,$$

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение.

$$0 = 0 * 1 + 0 * 2,$$

$$1 = 1 * 1 + 0 * 2,$$

$$2 = ? * 1 + ? * 2,$$

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение.

$$0 = 0 * 1 + 0 * 2,$$

$$1 = 1 * 1 + 0 * 2,$$

$$2 = 0 * 1 + 1 * 2,$$

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение.

$$0 = 0 * 1 + 0 * 2,$$

$$1 = 1 * 1 + 0 * 2,$$

$$2 = 0 * 1 + 1 * 2,$$

$$3 = ? * 1 + ? * 2.$$

Пример 2. В поле F операции заданы таблицами Кели.

$x + y$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$x * y$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Найдите многочлен минимальной степени над подполем $P = \{0; 1\}$, корнем которого является элемент 2.

Проверьте, что $\{2^0; 2\} = \{1; 2\}$ является базисом F , рассматриваемого как линейное пространство над P .

Решение.

$$0 = 0 * 1 + 0 * 2,$$

$$1 = 1 * 1 + 0 * 2,$$

$$2 = 0 * 1 + 1 * 2,$$

$$3 = 1 * 1 + 1 * 2.$$

[Вернуться к лекции?](#)

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$. **б)** Построить расширение этого поля с помощью корня s многочлена $x^3 + 2x^2 + x + 1$. Найти неприводимый многочлен минимальной степени, корнем которого является $(s - 1)$. **в)** Построить расширение этого поля с помощью корня b многочлена $x^3 + 2x^2 + 2x + 2$. Найти неприводимый многочлен минимальной степени, корнем которого является $(b + 1)$.

Решение.

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Решение. Что значит «построить поле»?

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Решение. Что значит «построить поле»? Мы должны представить искомое поле в *стандартном виде*. В данном случае это означает, что мы должны указать

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Решение. Что значит «построить поле»? Мы должны представить искомое поле в *стандартном виде*. В данном случае это означает, что мы должны указать носитель этого поля и каким-то образом задать операции. По критерию алгебраичности элемента система векторов $\{t^0; t; t^2\}$ является базисом искомого поля как линейного пространства над исходным полем.

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Решение. По критерию алгебраичности элемента система векторов $\{t^0; t; t^2\}$ является базисом искомого поля как линейного пространства над исходным полем. Значит, для случая **а)** носитель искомого поля имеет вид

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Решение. По критерию алгебраичности элемента система векторов $\{t^0; t; t^2\}$ является базисом искомого поля как линейного пространства над исходным полем. Значит, для случая **а)** носитель искомого поля имеет вид

$$\left\{ \alpha_0 + \alpha_1 t + \alpha_2 t^2 \mid \{\alpha_0; \alpha_1; \alpha_2\} \subseteq \{0; 1; 2\} \right\} =$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Решение. По критерию алгебраичности элемента система векторов $\{t^0; t; t^2\}$ является базисом искомого поля как линейного пространства над исходным полем. Значит, для случая **а)** носитель искомого поля имеет вид

$$\left\{ \alpha_0 + \alpha_1 t + \alpha_2 t^2 \mid \{\alpha_0; \alpha_1; \alpha_2\} \subseteq \{0; 1; 2\} \right\} =$$

$$= \{0; 1; 2; t; t + 1; t + 2; 2t; 2t + 1; 2t + 2; t^2; \dots; 2t^2 + 2t + 2\}$$

(всего ??? элементов).

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Решение. По критерию алгебраичности элемента система векторов $\{t^0; t; t^2\}$ является базисом искомого поля как линейного пространства над исходным полем. Значит, для случая **а)** носитель искомого поля имеет вид

$$\left\{ \alpha_0 + \alpha_1 t + \alpha_2 t^2 \mid \{\alpha_0; \alpha_1; \alpha_2\} \subseteq \{0; 1; 2\} \right\} =$$

$$= \{0; 1; 2; t; t + 1; t + 2; 2t; 2t + 1; 2t + 2; t^2; \dots; 2t^2 + 2t + 2\}$$

(всего 27 элементов).

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **б)** Построить расширение этого поля с помощью корня s многочлена $x^3 + 2x^2 + x + 1$. Найти неприводимый многочлен минимальной степени, корнем которого является $(s - 1)$.

Решение. Аналогично выглядит носитель искомого поля для случая б):

$$\left\{ \alpha_0 + \alpha_1 s + \alpha_2 s^2 \mid \{\alpha_0; \alpha_1; \alpha_2\} \subseteq \{0; 1; 2\} \right\},$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **в)** Построить расширение этого поля с помощью корня b многочлена $x^3 + 2x^2 + 2x + 2$. Найти неприводимый многочлен минимальной степени, корнем которого является $(b + 1)$.

Решение. Аналогично выглядит носитель искомого поля для случая **в)**:

$$\left\{ \alpha_0 + \alpha_1 b + \alpha_2 b^2 \mid \{\alpha_0; \alpha_1; \alpha_2\} \subseteq \{0; 1; 2\} \right\}.$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Решение. Операцию «сложение» проще всего задать

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Решение. Операцию «сложение» проще всего задать формулой, например, для случая **а)** имеем:

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$(\alpha_0 + \alpha_1 t + \alpha_2 t^2) + (\beta_0 + \beta_1 t + \beta_2 t^2) =$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned} &(\alpha_0 + \alpha_1 t + \alpha_2 t^2) + (\beta_0 + \beta_1 t + \beta_2 t^2) = \\ &= (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1) t + (\alpha_2 + \beta_2) t^2. \end{aligned}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Решение. Для задания операции «умножение» можно с успехом применить два подхода.

Во-первых, можно

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Решение. Для задания операции «умножение» можно с успехом применить два подхода.

Во-первых, можно задать эту операцию формулой.

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Решение. Для задания операции «умножение» можно с успехом применить два подхода.

Во-первых, можно задать эту операцию формулой.

Во-вторых, можно воспользоваться цикличностью мультипликативной группы поля Галуа.

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Решение. Сначала зададим операцию «умножение» в искомом расширении поля формулой.

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned}
 & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\
 & = \alpha_0 \beta_0 + (\quad) t + (\quad) t^2 + \\
 & \quad + (\quad) t^3 + \alpha_2 \beta_2 t^4 =
 \end{aligned}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned}
 & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\
 & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\quad) t^2 + \\
 & \quad + (\quad) t^3 + \alpha_2 \beta_2 t^4 =
 \end{aligned}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned}
 & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\
 & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\
 & \quad + (\quad \quad \quad) t^3 + \alpha_2 \beta_2 t^4 =
 \end{aligned}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned}
 & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\
 & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\
 & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) t^3 + \alpha_2 \beta_2 t^4 =
 \end{aligned}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned} & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\ & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\ & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) t^3 + \alpha_2 \beta_2 t^4 = \end{aligned}$$

Надо выразить t^3 и t^4 в виде $(\gamma_0 + \gamma_1 t + \gamma_2 t^2)$.

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned} & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\ & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\ & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) t^3 + \alpha_2 \beta_2 t^4 = \end{aligned}$$

Надо выразить t^3 и t^4 в виде $(\gamma_0 + \gamma_1 t + \gamma_2 t^2)$.

t — корень многочлена $x^3 + x^2 + 2$, поэтому

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned} & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\ & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\ & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) t^3 + \alpha_2 \beta_2 t^4 = \end{aligned}$$

Надо выразить t^3 и t^4 в виде $(\gamma_0 + \gamma_1 t + \gamma_2 t^2)$.

t — корень многочлена $x^3 + x^2 + 2$, поэтому

$$t^3 + t^2 + 2 = 0 \Rightarrow ???$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned} & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\ & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\ & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) t^3 + \alpha_2 \beta_2 t^4 = \end{aligned}$$

Надо выразить t^3 и t^4 в виде $(\gamma_0 + \gamma_1 t + \gamma_2 t^2)$.

t — корень многочлена $x^3 + x^2 + 2$, поэтому

$$t^3 + t^2 + 2 = 0 \Rightarrow ???$$

$$1 + 1 + 1 = 0 \Rightarrow$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned} & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\ & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\ & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) t^3 + \alpha_2 \beta_2 t^4 = \end{aligned}$$

Надо выразить t^3 и t^4 в виде $(\gamma_0 + \gamma_1 t + \gamma_2 t^2)$.

t — корень многочлена $x^3 + x^2 + 2$, поэтому

$$t^3 + t^2 + 2 = 0 \Rightarrow ???$$

$$1 + 1 + 1 = 0 \Rightarrow 1 + 2 = 2 + 1 = 0 \Rightarrow$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned} & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\ & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\ & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) t^3 + \alpha_2 \beta_2 t^4 = \end{aligned}$$

Надо выразить t^3 и t^4 в виде $(\gamma_0 + \gamma_1 t + \gamma_2 t^2)$.

t — корень многочлена $x^3 + x^2 + 2$, поэтому

$$t^3 + t^2 + 2 = 0 \Rightarrow ???$$

$$1 + 1 + 1 = 0 \Rightarrow 1 + 2 = 2 + 1 = 0 \Rightarrow \begin{cases} -1 = \\ -2 = \end{cases}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned} & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\ &= \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\ & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) t^3 + \alpha_2 \beta_2 t^4 = \end{aligned}$$

Надо выразить t^3 и t^4 в виде $(\gamma_0 + \gamma_1 t + \gamma_2 t^2)$.

t — корень многочлена $x^3 + x^2 + 2$, поэтому

$$t^3 + t^2 + 2 = 0 \Rightarrow ???$$

$$1 + 1 + 1 = 0 \Rightarrow 1 + 2 = 2 + 1 = 0 \Rightarrow \begin{cases} -1 = 2, \\ -2 = 1. \end{cases}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned} & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\ & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\ & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) t^3 + \alpha_2 \beta_2 t^4 = \end{aligned}$$

Надо выразить t^3 и t^4 в виде $(\gamma_0 + \gamma_1 t + \gamma_2 t^2)$.

t — корень многочлена $x^3 + x^2 + 2$, поэтому

$$t^3 + t^2 + 2 = 0 \Rightarrow t^3 = -t^2 - 2$$

$$1 + 1 + 1 = 0 \Rightarrow 1 + 2 = 2 + 1 = 0 \Rightarrow \begin{cases} -1 = 2, \\ -2 = 1. \end{cases}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned} & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\ & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\ & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) t^3 + \alpha_2 \beta_2 t^4 = \end{aligned}$$

Надо выразить t^3 и t^4 в виде $(\gamma_0 + \gamma_1 t + \gamma_2 t^2)$.

t — корень многочлена $x^3 + x^2 + 2$, поэтому

$$\begin{aligned} t^3 + t^2 + 2 &= 0 \Rightarrow t^3 = -t^2 - 2 \Rightarrow \\ \Rightarrow t^4 &= -t^3 - 2t^2 = \end{aligned}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned} & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\ & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\ & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) t^3 + \alpha_2 \beta_2 t^4 = \end{aligned}$$

Надо выразить t^3 и t^4 в виде $(\gamma_0 + \gamma_1 t + \gamma_2 t^2)$.

t — корень многочлена $x^3 + x^2 + 2$, поэтому

$$\begin{aligned} t^3 + t^2 + 2 &= 0 \Rightarrow t^3 = -t^2 - 2 \Rightarrow \\ \Rightarrow t^4 &= -t^3 - 2t = t^2 + 2t - 2 \end{aligned}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned} & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\ & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\ & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) t^3 + \alpha_2 \beta_2 t^4 = \end{aligned}$$

Надо выразить t^3 и t^4 в виде $(\gamma_0 + \gamma_1 t + \gamma_2 t^2)$.

t — корень многочлена $x^3 + x^2 + 2$, поэтому

$$\begin{aligned} t^3 + t^2 + 2 &= 0 \Rightarrow t^3 = -t^2 - 2 \Rightarrow \\ \Rightarrow t^4 &= -t^3 - 2 = -(-t^2 - 2) - 2 = t^2 + t + 2. \end{aligned}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned} & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\ & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\ & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) t^3 + \alpha_2 \beta_2 t^4 = \end{aligned}$$

$$\boxed{t^3 = 2t^2 + 1 \Rightarrow t^4 = t^2 + t + 2}$$

$$\begin{aligned} & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\ & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) \underbrace{(\quad)}_{t^3} + \alpha_2 \beta_2 \underbrace{(\quad)}_{t^4} = \end{aligned}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned} & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\ & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\ & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) t^3 + \alpha_2 \beta_2 t^4 = \end{aligned}$$

$$\boxed{t^3 = 2t^2 + 1 \Rightarrow t^4 = t^2 + t + 2}$$

$$\begin{aligned} & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\ & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) \underbrace{(2t^2 + 1)}_{t^3} + \alpha_2 \beta_2 \underbrace{(t^2 + t + 2)}_{t^4} = \end{aligned}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned}
 & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\
 & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\
 & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) t^3 + \alpha_2 \beta_2 t^4 = \\
 & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\
 & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) (2t^2 + 1) + \alpha_2 \beta_2 (t^2 + t + 2) = \\
 & = (\hspace{10em}) + (\hspace{10em}) t + \\
 & \quad + (\hspace{10em}) t^2.
 \end{aligned}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned}
 & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\
 & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\
 & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) t^3 + \alpha_2 \beta_2 t^4 = \\
 & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\
 & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) (2t^2 + 1) + \alpha_2 \beta_2 (t^2 + t + 2) = \\
 & = (\alpha_0 \beta_0 + \alpha_1 \beta_2 + \alpha_2 \beta_1 + 2\alpha_2 \beta_2) + (\quad) t + \\
 & \quad + (\quad) t^2.
 \end{aligned}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned}
 & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\
 & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\
 & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) t^3 + \alpha_2 \beta_2 t^4 = \\
 & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\
 & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) (2t^2 + 1) + \alpha_2 \beta_2 (t^2 + t + 2) = \\
 & = (\alpha_0 \beta_0 + \alpha_1 \beta_2 + \alpha_2 \beta_1 + 2\alpha_2 \beta_2) + (\alpha_0 \beta_1 + \alpha_1 \beta_0 + \alpha_2 \beta_2) t + \\
 & \quad + (\hspace{15em}) t^2.
 \end{aligned}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned}
 & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\
 & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\
 & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) t^3 + \alpha_2 \beta_2 t^4 = \\
 & = \alpha_0 \beta_0 + (\alpha_0 \beta_1 + \alpha_1 \beta_0) t + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) t^2 + \\
 & \quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1) (2t^2 + 1) + \alpha_2 \beta_2 (t^2 + t + 2) = \\
 & = (\alpha_0 \beta_0 + \alpha_1 \beta_2 + \alpha_2 \beta_1 + 2\alpha_2 \beta_2) + (\alpha_0 \beta_1 + \alpha_1 \beta_0 + \alpha_2 \beta_2) t + \\
 & \quad + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0 + 2\alpha_1 \beta_2 + 2\alpha_2 \beta_1 + \alpha_2 \beta_2) t^2.
 \end{aligned}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

$$\begin{aligned} & (\alpha_0 + \alpha_1 t + \alpha_2 t^2) (\beta_0 + \beta_1 t + \beta_2 t^2) = \\ & = (\alpha_0 \beta_0 + \alpha_1 \beta_2 + \alpha_2 \beta_1 + 2\alpha_2 \beta_2) + (\alpha_0 \beta_1 + \alpha_1 \beta_0 + \alpha_2 \beta_2) t + \\ & \quad + (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0 + 2\alpha_1 \beta_2 + 2\alpha_2 \beta_1 + \alpha_2 \beta_2) t^2. \end{aligned}$$

Итак, произведение задано формулой.

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Теперь реализуем второй подход к заданию операции «умножение», т.е. воспользуемся цикличностью поля. Если u — порождающий элемент мультипликативной группы искомого поля, то операцию «умножение» можно задать формулой

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Теперь реализуем второй подход к заданию операции «умножение», т.е. воспользуемся цикличностью поля. Если u — порождающий элемент мультипликативной группы искомого поля, то операцию «умножение» можно задать формулой

$$\begin{cases} u^k \cdot u^m = u^n; \\ 0 \cdot u^m = 0; \\ u^k \cdot 0 = 0, \end{cases} \quad \text{где } n \text{ — остаток от}$$

деления числа $(k + m)$ на 26 (напомним, что порядок мультипликативной группы равен $27 - 1$, где 27 — порядок¹ искомого поля).

¹Т.е. число элементов в носителе.

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Следовательно, для использования этой формулы во всех рассматриваемых случаях нам необходимо найти порождающий элемент циклической группы и представить все степени этого элемента в виде, соответственно, $(\alpha_0 + \alpha_1 t + \alpha_2 t^2)$, $(\alpha_0 + \alpha_1 s + \alpha_2 s^2)$ или $(\alpha_0 + \alpha_1 b + \alpha_2 b^2)$.

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

В исходном поле из равенства $1 + 1 + 1 = 0$ следует $(-2) =$ и $(-1) =$.

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

В исходном поле из равенства $1 + 1 + 1 = 0$ следует $(-2) = 1$ и $(-1) = 2$.

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

В исходном поле из равенства $1 + 1 + 1 = 0$ следует $(-2) = 1$ и $(-1) = 2$. Поэтому для случая **а)** из уравнения $t^3 + t^2 + 2 = 0$ получаем $t^3 = 2t^2 + 1$, для случая **б)** получаем

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

В исходном поле из равенства $1 + 1 + 1 = 0$ следует $(-2) = 1$ и $(-1) = 2$. Поэтому для случая **а)** из уравнения $t^3 + t^2 + 2 = 0$ получаем $t^3 = 2t^2 + 1$, для случая **б)** получаем $s^3 = s^2 + 2s + 2$, для случая **в)** —

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

В исходном поле из равенства $1 + 1 + 1 = 0$ следует $(-2) = 1$ и $(-1) = 2$. Поэтому для случая **а)** из уравнения $t^3 + t^2 + 2 = 0$ получаем $t^3 = 2t^2 + 1$, для случая **б)** получаем $s^3 = s^2 + 2s + 2$, для случая **в)** — $b^3 = s^2 + s + 1$.

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

В исходном поле из равенства $1 + 1 + 1 = 0$ следует $(-2) = 1$ и $(-1) = 2$. Поэтому для случая **а)** из уравнения $t^3 + t^2 + 2 = 0$ получаем $t^3 = 2t^2 + 1$. Следовательно, (учитывая, что в исходном поле, например, $2 \cdot 2 = 1$, $2 + 2 = 1$)

$$t^4 = t \cdot t^3 =$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

В исходном поле из равенства $1 + 1 + 1 = 0$ следует $(-2) = 1$ и $(-1) = 2$. Поэтому для случая **а)** из уравнения $t^3 + t^2 + 2 = 0$ получаем $t^3 = 2t^2 + 1$. Следовательно, (учитывая, что в исходном поле, например, $2 \cdot 2 = 1$, $2 + 2 = 1$)

$$t^4 = t \cdot t^3 = t \cdot (2t^2 + 1) =$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

В исходном поле из равенства $1 + 1 + 1 = 0$ следует $(-2) = 1$ и $(-1) = 2$. Поэтому для случая **а)** из уравнения $t^3 + t^2 + 2 = 0$ получаем $t^3 = 2t^2 + 1$. Следовательно, (учитывая, что в исходном поле, например, $2 \cdot 2 = 1$, $2 + 2 = 1$)

$$t^4 = t \cdot t^3 = t \cdot (2t^2 + 1) = 2(2t^2 + 1) + t =$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

В исходном поле из равенства $1 + 1 + 1 = 0$ следует $(-2) = 1$ и $(-1) = 2$. Поэтому для случая **а)** из уравнения $t^3 + t^2 + 2 = 0$ получаем $t^3 = 2t^2 + 1$. Следовательно, (учитывая, что в исходном поле, например, $2 \cdot 2 = 1$, $2 + 2 = 1$)

$$t^4 = t \cdot t^3 = t \cdot (2t^2 + 1) = 2(2t^2 + 1) + t = t^2 + t + 2,$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

В исходном поле из равенства $1 + 1 + 1 = 0$ следует $(-2) = 1$ и $(-1) = 2$. Поэтому для случая **а)** из уравнения $t^3 + t^2 + 2 = 0$ получаем $t^3 = 2t^2 + 1$. Следовательно, (учитывая, что в исходном поле, например, $2 \cdot 2 = 1$, $2 + 2 = 1$)

$$t^4 = t \cdot t^3 = t \cdot (2t^2 + 1) = 2(2t^2 + 1) + t = t^2 + t + 2,$$

$$t^5 =$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

В исходном поле из равенства $1 + 1 + 1 = 0$ следует $(-2) = 1$ и $(-1) = 2$. Поэтому для случая **а)** из уравнения $t^3 + t^2 + 2 = 0$ получаем $t^3 = 2t^2 + 1$. Следовательно, (учитывая, что в исходном поле, например, $2 \cdot 2 = 1$, $2 + 2 = 1$)

$$t^4 = t \cdot t^3 = t \cdot (2t^2 + 1) = 2(2t^2 + 1) + t = t^2 + t + 2,$$

$$t^5 = t \cdot t^4 =$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

В исходном поле из равенства $1 + 1 + 1 = 0$ следует $(-2) = 1$ и $(-1) = 2$. Поэтому для случая **а)** из уравнения $t^3 + t^2 + 2 = 0$ получаем $t^3 = 2t^2 + 1$. Следовательно, (учитывая, что в исходном поле, например, $2 \cdot 2 = 1$, $2 + 2 = 1$)

$$t^4 = t \cdot t^3 = t \cdot (2t^2 + 1) = 2(2t^2 + 1) + t = t^2 + t + 2,$$

$$t^5 = t \cdot t^4 = t \cdot (t^2 + t + 2) =$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

В исходном поле из равенства $1 + 1 + 1 = 0$ следует $(-2) = 1$ и $(-1) = 2$. Поэтому для случая **а)** из уравнения $t^3 + t^2 + 2 = 0$ получаем $t^3 = 2t^2 + 1$. Следовательно, (учитывая, что в исходном поле, например, $2 \cdot 2 = 1$, $2 + 2 = 1$)

$$t^4 = t \cdot t^3 = t \cdot (2t^2 + 1) = 2(2t^2 + 1) + t = t^2 + t + 2,$$

$$t^5 = t \cdot t^4 = t \cdot (t^2 + t + 2) = (2t^2 + 1) + t^2 + 2t =$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

В исходном поле из равенства $1 + 1 + 1 = 0$ следует $(-2) = 1$ и $(-1) = 2$. Поэтому для случая **а)** из уравнения $t^3 + t^2 + 2 = 0$ получаем $t^3 = 2t^2 + 1$. Следовательно, (учитывая, что в исходном поле, например, $2 \cdot 2 = 1$, $2 + 2 = 1$)

$$t^4 = t \cdot t^3 = t \cdot (2t^2 + 1) = 2(2t^2 + 1) + t = t^2 + t + 2,$$

$$t^5 = t \cdot t^4 = t \cdot (t^2 + t + 2) = (2t^2 + 1) + t^2 + 2t = 2t + 1 \dots$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

В исходном поле из равенства $1 + 1 + 1 = 0$ следует $(-2) = 1$ и $(-1) = 2$. Поэтому для случая **а)** из уравнения $t^3 + t^2 + 2 = 0$ получаем $t^3 = 2t^2 + 1$. Следовательно, (учитывая, что в исходном поле, например, $2 \cdot 2 = 1$, $2 + 2 = 1$)

$$t^4 = t \cdot t^3 = t \cdot (2t^2 + 1) = 2(2t^2 + 1) + t = t^2 + t + 2,$$

$$t^5 = t \cdot t^4 = t \cdot (t^2 + t + 2) = (2t^2 + 1) + t^2 + 2t = 2t + 1 \dots$$

Продолжив эти вычисления, получаем результаты, представленные в таблице **1**

Таблица 1.

n	t^n
1	t
2	t^2
3	$2t^2 + 1$
4	$t^2 + t + 2$
5	$2t + 1$
6	$2t^2 + t$
7	$2t^2 + 2$
8	$t^2 + 2t + 2$
9	$t^2 + 2t + 1$
10	$t^2 + t + 1$
11	$t + 1$
12	$t^2 + t$
13	1

n	s^n	n	s^n
1	s	14	$2s$
2	s^2	15	$2s^2$
3	$s^2 + 2s + 2$	16	$2s^2 + s + 1$
4	$s + 2$	17	$2s + 1$
5	$s^2 + 2s$	18	$2s^2 + s$
6	$2s + 2$	19	$s + 1$
7	$2s^2 + 2s$	20	$s^2 + s$
8	$s^2 + s + 1$	21	$2s^2 + 2s + 2$
9	$2s^2 + 2$	22	$s^2 + 1$
10	$2s^2 + 1$	23	$s^2 + 2$
11	$2s^2 + 2s + 1$	24	$s^2 + s + 2$
12	$s^2 + 2s + 1$	25	$2s^2 + s + 2$
13	2	26	1

n	b^n
1	b
2	b^2
3	$b^2 + b + 1$
4	$2b^2 + 2b + 1$
5	$b^2 + 2$
6	$b^2 + 1$
7	$b^2 + 2b + 1$
8	$2b + 1$
9	$2b^2 + b$
10	$2b + 2$
11	$2b^2 + 2b$
12	$b^2 + 2b + 2$
13	1

Описание поля в случае **б)** завершено. Но в случаях **а)** и **в)** все обстоит менее благополучно, поскольку элементы t и b не являются порождающими для мультипликативных групп искоемых полей.

Описание поля в случае **б)** завершено. Но в случаях **а)** и **в)** все обстоит менее благополучно, поскольку элементы t и b не являются порождающими для мультипликативных групп искомым полем. В рассматриваемом случае найти требуемые порождающие несложно. В самом деле, порядок элемента делит порядок группы. Значит, в мультипликативной группе искомого поля всякий элемент имеет порядок

Описание поля в случае **б)** завершено. Но в случаях **а)** и **в)** все обстоит менее благополучно, поскольку элементы t и b не являются порождающими для мультипликативных групп искоемых полей. В рассматриваемом случае найти требуемые порождающие несложно. В самом деле, порядок элемента делит порядок группы. Значит, в мультипликативной группе искомого поля всякий элемент имеет порядок 1, 2,

Описание поля в случае **б)** завершено. Но в случаях **а)** и **в)** все обстоит менее благополучно, поскольку элементы t и b не являются порождающими для мультипликативных групп искоемых полей. В рассматриваемом случае найти требуемые порождающие несложно. В самом деле, порядок элемента делит порядок группы. Значит, в мультипликативной группе искомого поля всякий элемент имеет порядок 1, 2, 13 или

Описание поля в случае **б)** завершено. Но в случаях **а)** и **в)** все обстоит менее благополучно, поскольку элементы t и b не являются порождающими для мультипликативных групп искомых полей. В рассматриваемом случае найти требуемые порождающие несложно. В самом деле, порядок элемента делит порядок группы. Значит, в мультипликативной группе искомого поля всякий элемент имеет порядок 1, 2, 13 или 26.

Описание поля в случае **б)** завершено. Но в случаях **а)** и **в)** все обстоит менее благополучно, поскольку элементы t и b не являются порождающими для мультипликативных групп искомым полем. В рассматриваемом случае найти требуемые порождающие несложно. В самом деле, порядок элемента делит порядок группы. Значит, в мультипликативной группе искомого поля всякий элемент имеет порядок 1, 2, 13 или 26.

Порядок 1 и 2 имеют только элементы исходного поля.

Описание поля в случае **б)** завершено. Но в случаях **а)** и **в)** все обстоит менее благополучно, поскольку элементы t и b не являются порождающими для мультипликативных групп искомым полем. В рассматриваемом случае найти требуемые порождающие несложно. В самом деле, порядок элемента делит порядок группы. Значит, в мультипликативной группе искомого поля всякий элемент имеет порядок 1, 2, 13 или 26.

Порядок 1 и 2 имеют только элементы исходного поля. Все элементы порядка 13 перечислены выше, они являются степенями элемента t и, соответственно, элемента b .

Описание поля в случае **б)** завершено. Но в случаях **а)** и **в)** все обстоит менее благополучно, поскольку элементы t и b не являются порождающими для мультипликативных групп искомым полем. В рассматриваемом случае найти требуемые порождающие несложно. В самом деле, порядок элемента делит порядок группы. Значит, в мультипликативной группе искомого поля всякий элемент имеет порядок 1, 2, 13 или 26.

Порядок 1 и 2 имеют только элементы исходного поля. Все элементы порядка 13 перечислены выше, они являются степенями элемента t и, соответственно, элемента b . Следовательно, для нахождения элемента, порождающего мультипликативную группу поля в случаях **а)** и **в)** нам достаточно выбрать элементы, не являющиеся степенями элементов t и, соответственно, b , и не лежащие в исходном поле.

Описание поля в случае **б)** завершено. Но в случаях **а)** и **в)** все обстоит менее благополучно, поскольку элементы t и b не являются порождающими для мультипликативных групп искомым полем. В рассматриваемом случае найти требуемые порождающие несложно. В самом деле, порядок элемента делит порядок группы. Значит, в мультипликативной группе искомого поля всякий элемент имеет порядок 1, 2, 13 или 26.

Порядок 1 и 2 имеют только элементы исходного поля. Все элементы порядка 13 перечислены выше, они являются степенями элемента t и, соответственно, элемента b . Следовательно, для нахождения элемента, порождающего мультипликативную группу поля в случаях **а)** и **в)** нам достаточно выбрать элементы, не являющиеся степенями элементов t и, соответственно, b , и не лежащие в исходном поле. Таковы, например, элементы $(t + 2)$ и $(b + 1)$.

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Имеем (учитывая, что в рассматриваемом поле $2 + 2 = 1$, $2 + 1 = 0$)

$$(t + 2)^2 =$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Имеем (учитывая, что в рассматриваемом поле $2 + 2 = 1$, $2 + 1 = 0$)

$$(t + 2)^2 = (t + 2)(t + 2) =$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Имеем (учитывая, что в рассматриваемом поле $2 + 2 = 1$, $2 + 1 = 0$)

$$(t + 2)^2 = (t + 2)(t + 2) = t^2 + t + 1,$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Имеем (учитывая, что в рассматриваемом поле $2 + 2 = 1$, $2 + 1 = 0$)

$$(t + 2)^2 = (t + 2)(t + 2) = t^2 + t + 1,$$

$$(t + 2)^3 =$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Имеем (учитывая, что в рассматриваемом поле $2 + 2 = 1$, $2 + 1 = 0$)

$$(t + 2)^2 = (t + 2)(t + 2) = t^2 + t + 1,$$

$$(t + 2)^3 = (t + 2) \cdot (t^2 + t + 1) =$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Имеем (учитывая, что в рассматриваемом поле $2 + 2 = 1$, $2 + 1 = 0$)

$$(t + 2)^2 = (t + 2)(t + 2) = t^2 + t + 1,$$

$$(t + 2)^3 = (t + 2) \cdot (t^2 + t + 1) = t^3 + 2 =$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Имеем (учитывая, что в рассматриваемом поле $2 + 2 = 1$, $2 + 1 = 0$)

$$(t + 2)^2 = (t + 2)(t + 2) = t^2 + t + 1,$$

$$(t + 2)^3 = (t + 2) \cdot (t^2 + t + 1) = t^3 + 2 = (2t^2 + 1) + 2 =$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Имеем (учитывая, что в рассматриваемом поле $2 + 2 = 1$, $2 + 1 = 0$)

$$(t + 2)^2 = (t + 2)(t + 2) = t^2 + t + 1,$$

$$(t + 2)^3 = (t + 2) \cdot (t^2 + t + 1) = t^3 + 2 = (2t^2 + 1) + 2 = 2t^2 \dots$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **а)** Построить расширение этого поля с помощью корня t многочлена $x^3 + x^2 + 2$. Найти все степени элемента t . Найти неприводимый многочлен минимальной степени, корнем которого является $(t + 2)$.

Имеем (учитывая, что в рассматриваемом поле $2 + 2 = 1$, $2 + 1 = 0$)

$$(t + 2)^2 = (t + 2)(t + 2) = t^2 + t + 1,$$

$$(t + 2)^3 = (t + 2) \cdot (t^2 + t + 1) = t^3 + 2 = (2t^2 + 1) + 2 = 2t^2 \dots$$

Продолжая таким же образом, получаем результат, представленный в таблице **2**.

Таблица 2.

n	$(t+2)^n$	n	$(t+2)^n$
1	$t+2$	14	$2t+1$
2	t^2+t+1	15	$2t^2+2t+2$
3	$2t^2$	16	t^2
4	$2t^2+2$	17	t^2+1
5	$2t^2+2t$	18	t^2+t
6	t^2+t+2	19	$2t^2+2t+1$
7	$2t^2+t+2$	20	t^2+2t+1
8	t	21	$2t$
9	t^2+2t	22	$2t^2+t$
10	$t+1$	23	$2t+2$
11	t^2+2	24	$2t^2+1$
12	t^2+2t+2	25	$2t^2+t+1$
13	2	26	1

n	$(b+1)^n$	n	$(b+1)^n$
1	$b+1$	14	$2b+2$
2	b^2+2b+1	15	$2b^2+b+2$
3	b^2+b+2	16	$2b^2+2b+1$
4	b	17	$2b$
5	b^2+b	18	$2b^2+2b$
6	$2b+1$	19	$b+2$
7	$2b^2+1$	20	b^2+2
8	b^2	21	$2s^2+2s+2$
9	$2b^2+b+1$	22	$2b^2$
10	$2b^2+b$	23	b^2+2b
11	$2b^2+b$	24	b^2+1
12	b^2+b+1	25	$2b^2+2b+2$
13	2	26	1

Найдем минимальный многочлен, корнем которого является элемент $(t + 2)$.

Найдем минимальный многочлен, корнем которого является элемент $(t + 2)$.

Естественно применить **стратегию составления уравнений**.

Найдем минимальный многочлен, корнем которого является элемент $(t + 2)$.

Что надо найти?

Найдем минимальный многочлен, корнем которого является элемент $(t + 2)$.

Что надо найти? Многочлен.

Найдем минимальный многочлен, корнем которого является элемент $(t + 2)$.

Что надо найти? Многочлен.

В каком виде представим ответ?

Найдем минимальный многочлен, корнем которого является элемент $(t + 2)$.

Что надо найти? Многочлен.

В каком виде представим ответ? В виде выражения от некоторой переменной.

Найдем минимальный многочлен, корнем которого является элемент $(t + 2)$.

Что надо найти? Многочлен.

В каком виде представим ответ? В виде выражения от некоторой переменной.

Введем переменные.

Найдем минимальный многочлен, корнем которого является элемент $(t + 2)$.

Что надо найти? Многочлен.

В каком виде представим ответ? В виде выражения от некоторой переменной.

Введем переменные. Обозначим буквами коэффициенты искомого уравнения и введем переменную x .

Найдем минимальный многочлен, корнем которого является элемент $(t + 2)$.

Что надо найти? Многочлен.

В каком виде представим ответ? В виде выражения от некоторой переменной.

Введем переменные. Обозначим буквами коэффициенты искомого уравнения и введем переменную x .

Искомый многочлен имеет вид $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + x^3$.

Найдем минимальный многочлен, корнем которого является элемент $(t + 2)$.

Что надо найти? Многочлен.

В каком виде представим ответ? В виде выражения от некоторой переменной.

Введем переменные. Обозначим буквами коэффициенты искомого уравнения и введем переменную x .

Искомый многочлен имеет вид $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + x^3$.

Составим уравнение. Значение какой величины вычислим двумя способами?

Найдем минимальный многочлен, корнем которого является элемент $(t + 2)$.

Что надо найти? Многочлен.

В каком виде представим ответ? В виде выражения от некоторой переменной.

Введем переменные. Обозначим буквами коэффициенты искомого уравнения и введем переменную x .

Искомый многочлен имеет вид $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + x^3$.

Составим уравнение. Значение какой величины вычислим двумя способами? Переведем на язык равенств утверждение о том, что $(t + 2)$ является корнем:

Найдем минимальный многочлен, корнем которого является элемент $(t + 2)$.

Что надо найти? Многочлен.

В каком виде представим ответ? В виде выражения от некоторой переменной.

Введем переменные. Обозначим буквами коэффициенты искомого уравнения и введем переменную x .

Искомый многочлен имеет вид $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + x^3$.

Составим уравнение. Значение какой величины вычислим двумя способами? Переведем на язык равенств утверждение о том, что $(t + 2)$ является корнем:

$$\alpha_0 + \alpha_1(t + 2) + \alpha_2(t + 2)^2 + (t + 2)^3 = 0.$$

Найдем минимальный многочлен, корнем которого является элемент $(t + 2)$.

Что надо найти? Многочлен.

В каком виде представим ответ? В виде выражения от некоторой переменной.

Введем переменные. Обозначим буквами коэффициенты искомого уравнения и введем переменную x .

Искомый многочлен имеет вид $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + x^3$.

Составим уравнение. Значение какой величины вычислим двумя способами? Переведем на язык равенств утверждение о том, что $(t + 2)$ является корнем:

$$\alpha_0 + \alpha_1(t + 2) + \alpha_2(\mathbf{t + 2})^2 + (\mathbf{t + 2})^3 = 0.$$

Найдем минимальный многочлен, корнем которого является элемент $(t + 2)$.

Что надо найти? Многочлен.

В каком виде представим ответ? В виде выражения от некоторой переменной.

Введем переменные. Обозначим буквами коэффициенты искомого уравнения и введем переменную x .

Искомый многочлен имеет вид $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + x^3$.

Составим уравнение. Значение какой величины вычислим двумя способами? Переведем на язык равенств утверждение о том, что $(t + 2)$ является корнем:

$$\alpha_0 + \alpha_1(t + 2) + \alpha_2(\mathbf{t + 2})^2 + (\mathbf{t + 2})^3 = 0.$$

Используя **таблицу 2**, (см. **вверху страницы**) получаем

Найдем минимальный многочлен, корнем которого является элемент $(t + 2)$.

Что надо найти? Многочлен.

В каком виде представим ответ? В виде выражения от некоторой переменной.

Введем переменные. Обозначим буквами коэффициенты искомого уравнения и введем переменную x .

Искомый многочлен имеет вид $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + x^3$.

Составим уравнение. Значение какой величины вычислим двумя способами? Переведем на язык равенств утверждение о том, что $(t + 2)$ является корнем:

$$\alpha_0 + \alpha_1(t + 2) + \alpha_2(\mathbf{t + 2})^2 + (\mathbf{t + 2})^3 = 0.$$

Используя **таблицу 2**, (см. **вверху страницы**) получаем

$$\alpha_0 + \alpha_1(t + 2) + \alpha_2 \underbrace{(\mathbf{t^2 + t + 1})}_{(t+2)^2} + \underbrace{\mathbf{2t^2}}_{(t+2)^3} = 0.$$

Для многочлена $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + x^3$ получили тождество

$$\alpha_0 + \alpha_1(t + 2) + \alpha_2(t^2 + t + 1) + 2t^2 = 0.$$

Для многочлена $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + x^3$ получили тождество

$$\alpha_0 + \alpha_1(t + \mathbf{2}) + \alpha_2(t^2 + t + \mathbf{1}) + 2t^2 = 0.$$

Сравнивая коэффициенты перед t^0 в левой и правой частях последнего равенства, получаем

{

Для многочлена $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + x^3$ получили тождество

$$\alpha_0 + \alpha_1(t + 2) + \alpha_2(t^2 + t + 1) + 2t^2 = 0.$$

Сравнивая коэффициенты перед t^0 в левой и правой частях последнего равенства, получаем

$$\left\{ \begin{array}{l} \alpha_0 + 2\alpha_1 + \alpha_2 = 0; \\ \end{array} \right.$$

Для многочлена $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + x^3$ получили тождество

$$\alpha_0 + \alpha_1(\mathbf{1}t + 2) + \alpha_2(t^2 + \mathbf{1}t + 1) + 2t^2 = 0.$$

Сравнивая коэффициенты перед t в левой и правой частях последнего равенства, получаем

$$\left\{ \begin{array}{l} \alpha_0 + 2\alpha_1 + \alpha_2 = 0; \\ \end{array} \right.$$

Для многочлена $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + x^3$ получили тождество

$$\alpha_0 + \alpha_1(\mathbf{1}t + 2) + \alpha_2(t^2 + \mathbf{1}t + 1) + 2t^2 = 0.$$

Сравнивая коэффициенты перед t в левой и правой частях последнего равенства, получаем

$$\begin{cases} \alpha_0 + 2\alpha_1 + \alpha_2 = 0; \\ \alpha_1 + \alpha_2 = 0; \end{cases}$$

Для многочлена $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + x^3$ получили тождество

$$\alpha_0 + \alpha_1(t + 2) + \textcolor{violet}{\alpha}_2(\textcolor{violet}{1}t^2 + t + 1) + \textcolor{violet}{2}t^2 = 0.$$

Сравнивая коэффициенты перед t^2 в левой и правой частях последнего равенства, получаем

$$\left\{ \begin{array}{l} \alpha_0 + 2\alpha_1 + \alpha_2 = 0; \\ \alpha_1 + \alpha_2 = 0; \end{array} \right.$$

Для многочлена $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + x^3$ получили тождество

$$\alpha_0 + \alpha_1(t + 2) + \alpha_2(1t^2 + t + 1) + 2t^2 = 0.$$

Сравнивая коэффициенты перед t^2 в левой и правой частях последнего равенства, получаем

$$\begin{cases} \alpha_0 + 2\alpha_1 + \alpha_2 = 0; \\ \alpha_1 + \alpha_2 = 0; \\ \alpha_2 + 2 = 0, \end{cases}$$

Для многочлена $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + x^3$ получили тождество

$$\alpha_0 + \alpha_1(t + 2) + \textcolor{violet}{\alpha}_2(\textcolor{violet}{1}t^2 + t + 1) + \textcolor{violet}{2}t^2 = 0.$$

Сравнивая коэффициенты перед t^2 в левой и правой частях последнего равенства, получаем

$$\begin{cases} \alpha_0 + 2\alpha_1 + \alpha_2 = 0; \\ \alpha_1 + \alpha_2 = 0; \\ \alpha_2 + 2 = 0, \end{cases} \Rightarrow \begin{cases} \alpha_0 = \\ \alpha_1 = \\ \alpha_2 = \end{cases}$$

Для многочлена $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + x^3$ получили тождество

$$\alpha_0 + \alpha_1(t + 2) + \alpha_2(t^2 + t + 1) + 2t^2 = 0.$$

Сравнивая коэффициенты перед t^k в левой и правой частях последнего равенства, получаем систему

$$\begin{cases} \alpha_0 + 2\alpha_1 + \alpha_2 = 0; \\ \alpha_1 + \alpha_2 = 0; \\ \alpha_2 + 2 = 0, \end{cases} \Rightarrow \begin{cases} \alpha_0 = 1; \\ \alpha_1 = 2; \\ \alpha_2 = 1. \end{cases}$$

Для многочлена $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + x^3$ получили тождество

$$\alpha_0 + \alpha_1(t+2) + \alpha_2(t^2 + t + 1) + 2t^2 = 0.$$

Сравнивая коэффициенты перед t^k в левой и правой частях последнего равенства, получаем систему

$$\begin{cases} \alpha_0 + 2\alpha_1 + \alpha_2 = 0; \\ \alpha_1 + \alpha_2 = 0; \\ \alpha_2 + 2 = 0, \end{cases} \Rightarrow \begin{cases} \alpha_0 = 1; \\ \alpha_1 = 2; \\ \alpha_2 = 1. \end{cases}$$

Следовательно, элемент $(t+2)$ является корнем многочлена

Для многочлена $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + x^3$ получили тождество

$$\alpha_0 + \alpha_1(t + 2) + \alpha_2(t^2 + t + 1) + 2t^2 = 0.$$

Сравнивая коэффициенты перед t^k в левой и правой частях последнего равенства, получаем систему

$$\begin{cases} \alpha_0 + 2\alpha_1 + \alpha_2 = 0; \\ \alpha_1 + \alpha_2 = 0; \\ \alpha_2 + 2 = 0, \end{cases} \Rightarrow \begin{cases} \alpha_0 = 1; \\ \alpha_1 = 2; \\ \alpha_2 = 1. \end{cases}$$

Следовательно, элемент $(t + 2)$ является корнем многочлена

$$1 + 2x + x^2 + x^3.$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **в)** Построить расширение этого поля с помощью корня b многочлена $x^3 + 2x^2 + 2x + 2$. Найти неприводимый многочлен минимальной степени, корнем которого является $(b + 1)$.

Решение. Пусть элемент $(b + 1)$ является корнем многочлена

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **в)** Построить расширение этого поля с помощью корня b многочлена $x^3 + 2x^2 + 2x + 2$. Найти неприводимый многочлен минимальной степени, корнем которого является $(b + 1)$.

Решение. Пусть элемент $(b + 1)$ является корнем многочлена

$$\beta_0 + \beta_1 x + \beta_2 x^2 + x^3 :$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **в)** Построить расширение этого поля с помощью корня b многочлена $x^3 + 2x^2 + 2x + 2$. Найти неприводимый многочлен минимальной степени, корнем которого является $(b + 1)$.

Решение. Пусть элемент $(b + 1)$ является корнем многочлена

$$\beta_0 + \beta_1 x + \beta_2 x^2 + x^3 : \quad \beta_0 + \beta_1(b + 1) + \beta_2(b + 1)^2 + (b + 1)^3 = 0.$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **в)** Построить расширение этого поля с помощью корня b многочлена $x^3 + 2x^2 + 2x + 2$. Найти неприводимый многочлен минимальной степени, корнем которого является $(b + 1)$.

Решение. Пусть элемент $(b + 1)$ является корнем многочлена

$$\beta_0 + \beta_1 x + \beta_2 x^2 + x^3 : \quad \beta_0 + \beta_1(b + 1) + \beta_2(b + 1)^2 + (b + 1)^3 = 0.$$

Используем равенства из **таблицы 2**

$$(b + 1)^2 = b^2 + 2b + 1, \quad (b + 1)^3 = b^2 + b + 2:$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **в)** Построить расширение этого поля с помощью корня b многочлена $x^3 + 2x^2 + 2x + 2$. Найти неприводимый многочлен минимальной степени, корнем которого является $(b + 1)$.

Решение. Пусть элемент $(b + 1)$ является корнем многочлена

$$\beta_0 + \beta_1 x + \beta_2 x^2 + x^3 : \quad \beta_0 + \beta_1(b + 1) + \beta_2(b + 1)^2 + (b + 1)^3 = 0.$$

Используем равенства из **таблицы 2**

$$(b + 1)^2 = b^2 + 2b + 1, \quad (b + 1)^3 = b^2 + b + 2:$$

$$\beta_0 + \beta_1(b+1) + \beta_2 \underbrace{(b^2 + 2b + 1)}_{(b+1)^2} + \underbrace{(b^2 + b + 2)}_{(b+1)^3} = 0$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **в)** Построить расширение этого поля с помощью корня b многочлена $x^3 + 2x^2 + 2x + 2$. Найти неприводимый многочлен минимальной степени, корнем которого является $(b + 1)$.

Решение. Пусть элемент $(b + 1)$ является корнем многочлена

$$\beta_0 + \beta_1 x + \beta_2 x^2 + x^3 : \quad \beta_0 + \beta_1(b + 1) + \beta_2(b + 1)^2 + (b + 1)^3 = 0.$$

Используем равенства из **таблицы 2**

$$(b + 1)^2 = b^2 + 2b + 1, \quad (b + 1)^3 = b^2 + b + 2:$$

$$\beta_0 + \beta_1(b+1) + \beta_2 (b^2 + 2b + 1) + (b^2 + b + 2) = 0 \Rightarrow \left\{ \right.$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **в)** Построить расширение этого поля с помощью корня b многочлена $x^3 + 2x^2 + 2x + 2$. Найти неприводимый многочлен минимальной степени, корнем которого является $(b + 1)$.

Решение. Пусть элемент $(b + 1)$ является корнем многочлена

$$\beta_0 + \beta_1 x + \beta_2 x^2 + x^3 : \quad \beta_0 + \beta_1(b + 1) + \beta_2(b + 1)^2 + (b + 1)^3 = 0.$$

Используем равенства из **таблицы 2**

$$(b + 1)^2 = b^2 + 2b + 1, \quad (b + 1)^3 = b^2 + b + 2:$$

$$\beta_0 + \beta_1(b+1) + \beta_2(b^2 + 2b + 1) + (b^2 + b + 2) = 0 \Rightarrow \begin{cases} \beta_0 + \beta_1 + \beta_2 + 2 = 0, \end{cases}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **в)** Построить расширение этого поля с помощью корня b многочлена $x^3 + 2x^2 + 2x + 2$. Найти неприводимый многочлен минимальной степени, корнем которого является $(b + 1)$.

Решение. Пусть элемент $(b + 1)$ является корнем многочлена

$$\beta_0 + \beta_1 x + \beta_2 x^2 + x^3 : \quad \beta_0 + \beta_1(b + 1) + \beta_2(b + 1)^2 + (b + 1)^3 = 0.$$

Используем равенства из **таблицы 2**

$$(b + 1)^2 = b^2 + 2b + 1, \quad (b + 1)^3 = b^2 + b + 2:$$

$$\beta_0 + \beta_1(b+1) + \beta_2(b^2 + 2b + 1) + (b^2 + b + 2) = 0 \Rightarrow \begin{cases} \beta_0 + \beta_1 + \beta_2 + 2 = 0, \\ \beta_1 + 2\beta_2 + 1 = 0, \end{cases}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **в)** Построить расширение этого поля с помощью корня b многочлена $x^3 + 2x^2 + 2x + 2$. Найти неприводимый многочлен минимальной степени, корнем которого является $(b + 1)$.

Решение. Пусть элемент $(b + 1)$ является корнем многочлена

$$\beta_0 + \beta_1 x + \beta_2 x^2 + x^3 : \quad \beta_0 + \beta_1(b + 1) + \beta_2(b + 1)^2 + (b + 1)^3 = 0.$$

Используем равенства из **таблицы 2**

$$(b + 1)^2 = b^2 + 2b + 1, \quad (b + 1)^3 = b^2 + b + 2:$$

$$\beta_0 + \beta_1(b+1) + \beta_2(b^2 + 2b + 1) + (b^2 + b + 2) = 0 \Rightarrow \begin{cases} \beta_0 + \beta_1 + \beta_2 + 2 = 0, \\ \beta_1 + 2\beta_2 + 1 = 0, \\ \beta_2 + 1 = 0, \end{cases}$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **в)** Построить расширение этого поля с помощью корня b многочлена $x^3 + 2x^2 + 2x + 2$. Найти неприводимый многочлен минимальной степени, корнем которого является $(b + 1)$.

Решение. Пусть элемент $(b + 1)$ является корнем многочлена

$$\beta_0 + \beta_1 x + \beta_2 x^2 + x^3 : \quad \beta_0 + \beta_1(b + 1) + \beta_2(b + 1)^2 + (b + 1)^3 = 0.$$

Используем равенства из **таблицы 2**

$$(b + 1)^2 = b^2 + 2b + 1, \quad (b + 1)^3 = b^2 + b + 2:$$

$$\beta_0 + \beta_1(b+1) + \beta_2(b^2 + 2b + 1) + (b^2 + b + 2) = 0 \Rightarrow \begin{cases} \beta_0 + \beta_1 + \beta_2 + 2 = 0, \\ \beta_1 + 2\beta_2 + 1 = 0, \\ \beta_2 + 1 = 0, \end{cases}$$

Следовательно, элемент $(b + 1)$ является корнем многочлена

$$\beta_0 + \beta_1 x + \beta_2 x^2 + x^3.$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **в)** Построить расширение этого поля с помощью корня b многочлена $x^3 + 2x^2 + 2x + 2$. Найти неприводимый многочлен минимальной степени, корнем которого является $(b + 1)$.

Решение. Пусть элемент $(b + 1)$ является корнем многочлена

$$\beta_0 + \beta_1 x + \beta_2 x^2 + x^3 : \quad \beta_0 + \beta_1(b + 1) + \beta_2(b + 1)^2 + (b + 1)^3 = 0.$$

Используем равенства из **таблицы 2**

$$(b + 1)^2 = b^2 + 2b + 1, \quad (b + 1)^3 = b^2 + b + 2:$$

$$\beta_0 + \beta_1(b+1) + \beta_2(b^2 + 2b + 1) + (b^2 + b + 2) = 0 \Rightarrow \begin{cases} \beta_0 + \beta_1 + \beta_2 + 2 = 0, \\ \beta_1 + 2\beta_2 + 1 = 0, \\ \beta_2 + 1 = 0, \end{cases}$$

Следовательно, элемент $(b + 1)$ является корнем многочлена

$$\beta_0 + \beta_1 x + 2x^2 + x^3.$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **в)** Построить расширение этого поля с помощью корня b многочлена $x^3 + 2x^2 + 2x + 2$. Найти неприводимый многочлен минимальной степени, корнем которого является $(b + 1)$.

Решение. Пусть элемент $(b + 1)$ является корнем многочлена

$$\beta_0 + \beta_1 x + \beta_2 x^2 + x^3 : \quad \beta_0 + \beta_1(b + 1) + \beta_2(b + 1)^2 + (b + 1)^3 = 0.$$

Используем равенства из **таблицы 2**

$$(b + 1)^2 = b^2 + 2b + 1, \quad (b + 1)^3 = b^2 + b + 2:$$

$$\beta_0 + \beta_1(b+1) + \beta_2 (b^2 + 2b + 1) + (b^2 + b + 2) = 0 \Rightarrow \begin{cases} \beta_0 + \beta_1 + \beta_2 + 2 = 0, \\ \beta_1 + 2\beta_2 + 1 = 0, \\ \beta_2 + 1 = 0, \end{cases}$$

Следовательно, элемент $(b + 1)$ является корнем многочлена

$$\beta_0 + x + 2x^2 + x^3.$$

Пример 3. Рассмотрим поле с носителем $\{0; 1; 2\}$. **в)** Построить расширение этого поля с помощью корня b многочлена $x^3 + 2x^2 + 2x + 2$. Найти неприводимый многочлен минимальной степени, корнем которого является $(b + 1)$.

Решение. Пусть элемент $(b + 1)$ является корнем многочлена

$$\beta_0 + \beta_1 x + \beta_2 x^2 + x^3 : \quad \beta_0 + \beta_1(b + 1) + \beta_2(b + 1)^2 + (b + 1)^3 = 0.$$

Используем равенства из **таблицы 2**

$$(b + 1)^2 = b^2 + 2b + 1, \quad (b + 1)^3 = b^2 + b + 2:$$

$$\beta_0 + \beta_1(b+1) + \beta_2(b^2 + 2b + 1) + (b^2 + b + 2) = 0 \Rightarrow \begin{cases} \beta_0 + \beta_1 + \beta_2 + 2 = 0, \\ \beta_1 + 2\beta_2 + 1 = 0, \\ \beta_2 + 1 = 0, \end{cases}$$

Следовательно, элемент $(b + 1)$ является корнем многочлена

$$1 + x + 2x^2 + x^3.$$

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение.

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Как и в решении **примера 3**, носитель представим в виде множества выражений вида

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Как и в решении **примера 3**, носитель представим в виде множества выражений вида

$$\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4.$$

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Как и в решении **примера 3**, носитель представим в виде множества выражений вида

$$\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4.$$

Операцию «сложение» зададим формулой

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Как и в решении **примера 3**, носитель представим в виде множества выражений вида

$$\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4.$$

Операцию «сложение» зададим формулой

$$(\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) + (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) =$$

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Как и в решении **примера 3**, носитель представим в виде множества выражений вида

$$\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4.$$

Операцию «сложение» зададим формулой

$$\begin{aligned} & (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) + (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \\ & = (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1) u + (\alpha_2 + \beta_2) u^2 + (\alpha_3 + \beta_3) u^3 + (\alpha_4 + \beta_4) u^4. \end{aligned}$$

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Как и в решении **примера 3**, носитель представим в виде множества выражений вида

$$\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4.$$

Для получения формулы, с помощью которой можно задать произведение в поле Q :

$$(\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \dots$$

вычислим u^5 , u^6 , u^7 и u^8 .

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Как и в решении **примера 3**, носитель представим в виде множества выражений вида

$$\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4.$$

Для получения формулы, с помощью которой можно задать произведение в поле Q :

$$\begin{aligned} (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \dots \\ 1 + u^2 + u^5 = 0 \Rightarrow \end{aligned}$$

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Как и в решении **примера 3**, носитель представим в виде множества выражений вида

$$\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4.$$

Для получения формулы, с помощью которой можно задать произведение в поле Q :

$$\begin{aligned} (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \dots \\ 1 + u^2 + u^5 = 0 \Rightarrow u^5 = \end{aligned}$$

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Как и в решении **примера 3**, носитель представим в виде множества выражений вида

$$\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4.$$

Для получения формулы, с помощью которой можно задать произведение в поле Q :

$$\begin{aligned} (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \dots \\ 1 + u^2 + u^5 = 0 \Rightarrow u^5 = u^2 + 1. \end{aligned}$$

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Как и в решении **примера 3**, носитель представим в виде множества выражений вида

$$\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4.$$

Для получения формулы, с помощью которой можно задать произведение в поле Q :

$$\begin{aligned} (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \dots \\ u^5 = u^2 + 1 \Rightarrow u^6 = \end{aligned}$$

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Как и в решении **примера 3**, носитель представим в виде множества выражений вида

$$\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4.$$

Для получения формулы, с помощью которой можно задать произведение в поле Q :

$$\begin{aligned} (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \dots \\ u^5 = u^2 + 1 \Rightarrow u^6 = u^3 + u \Rightarrow \end{aligned}$$

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Как и в решении **примера 3**, носитель представим в виде множества выражений вида

$$\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4.$$

Для получения формулы, с помощью которой можно задать произведение в поле Q :

$$\begin{aligned} (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \dots \\ u^5 = u^2 + 1 \Rightarrow u^6 = u^3 + u \Rightarrow u^7 = \end{aligned}$$

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Как и в решении **примера 3**, носитель представим в виде множества выражений вида

$$\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4.$$

Для получения формулы, с помощью которой можно задать произведение в поле Q :

$$\begin{aligned} (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \dots \\ u^5 = u^2 + 1 \Rightarrow u^6 = u^3 + u \Rightarrow u^7 = u^4 + u^2 \Rightarrow \end{aligned}$$

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Как и в решении **примера 3**, носитель представим в виде множества выражений вида

$$\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4.$$

Для получения формулы, с помощью которой можно задать произведение в поле Q :

$$(\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \dots$$

$$u^5 = u^2 + 1 \Rightarrow u^6 = u^3 + u \Rightarrow u^7 = u^4 + u^2 \Rightarrow$$

$$\Rightarrow u^8 =$$

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Как и в решении **примера 3**, носитель представим в виде множества выражений вида

$$\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4.$$

Для получения формулы, с помощью которой можно задать произведение в поле Q :

$$(\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \dots$$

$$u^5 = u^2 + 1 \Rightarrow u^6 = u^3 + u \Rightarrow u^7 = u^4 + u^2 \Rightarrow$$

$$\Rightarrow u^8 = u^5 + u^3 =$$

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Как и в решении **примера 3**, носитель представим в виде множества выражений вида

$$\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4.$$

Для получения формулы, с помощью которой можно задать произведение в поле Q :

$$(\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \dots$$

$$u^5 = u^2 + 1 \Rightarrow u^6 = u^3 + u \Rightarrow u^7 = u^4 + u^2 \Rightarrow$$

$$\Rightarrow u^8 = u^5 + u^3 = u^2 + 1 + u^3.$$

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. $Q : \quad \alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4$.

$$u^5 = u^2 + 1 \Rightarrow u^6 = u^3 + u \Rightarrow u^7 = u^4 + u^2 \Rightarrow u^8 = u^3 + u^2 + 1.$$

$$\begin{aligned} & (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \\ & = \alpha_0 \beta_0 + u (\alpha_0 \beta_1 + \alpha_1 \beta_0) + u^2 (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) + \\ & + u^3 (\alpha_0 \beta_3 + \alpha_1 \beta_2 + \alpha_2 \beta_1 + \alpha_3 \beta_0) + u^4 (\alpha_0 \beta_4 + \alpha_1 \beta_3 + \alpha_2 \beta_2 + \alpha_3 \beta_1 + \alpha_4 \beta_0) + \\ & + u^5 (\alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1) + u^6 (\alpha_2 \beta_4 + \alpha_3 \beta_3 + \alpha_4 \beta_2) + \\ & + u^7 (\alpha_3 \beta_4 + \alpha_4 \beta_3) + \alpha_4 \beta_4 u^8. \end{aligned}$$

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. $Q : \quad \alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4$.

$$u^5 = u^2 + 1 \Rightarrow u^6 = u^3 + u \Rightarrow u^7 = u^4 + u^2 \Rightarrow u^8 = u^3 + u^2 + 1.$$

$$\begin{aligned} & (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \\ & = \alpha_0 \beta_0 + u (\alpha_0 \beta_1 + \alpha_1 \beta_0) + u^2 (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) + \\ & + u^3 (\alpha_0 \beta_3 + \alpha_1 \beta_2 + \alpha_2 \beta_1 + \alpha_3 \beta_0) + u^4 (\alpha_0 \beta_4 + \alpha_1 \beta_3 + \alpha_2 \beta_2 + \alpha_3 \beta_1 + \alpha_4 \beta_0) + \\ & + (u^2 + 1) (\alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1) + u^6 (\alpha_2 \beta_4 + \alpha_3 \beta_3 + \alpha_4 \beta_2) + \\ & + u^7 (\alpha_3 \beta_4 + \alpha_4 \beta_3) + \alpha_4 \beta_4 u^8. \end{aligned}$$

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. $Q : \quad \alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4$.

$$u^5 = u^2 + 1 \Rightarrow u^6 = u^3 + u \Rightarrow u^7 = u^4 + u^2 \Rightarrow u^8 = u^3 + u^2 + 1.$$

$$\begin{aligned} & (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \\ & = \alpha_0 \beta_0 + u (\alpha_0 \beta_1 + \alpha_1 \beta_0) + u^2 (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) + \\ & + u^3 (\alpha_0 \beta_3 + \alpha_1 \beta_2 + \alpha_2 \beta_1 + \alpha_3 \beta_0) + u^4 (\alpha_0 \beta_4 + \alpha_1 \beta_3 + \alpha_2 \beta_2 + \alpha_3 \beta_1 + \alpha_4 \beta_0) + \\ & + (u^2 + 1) (\alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1) + (u^3 + u) (\alpha_2 \beta_4 + \alpha_3 \beta_3 + \alpha_4 \beta_2) + \\ & + u^7 (\alpha_3 \beta_4 + \alpha_4 \beta_3) + \alpha_4 \beta_4 u^8. \end{aligned}$$

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. $Q : \quad \alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4$.

$$u^5 = u^2 + 1 \Rightarrow u^6 = u^3 + u \Rightarrow u^7 = u^4 + u^2 \Rightarrow u^8 = u^3 + u^2 + 1.$$

$$\begin{aligned} & (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \\ & = \alpha_0 \beta_0 + u (\alpha_0 \beta_1 + \alpha_1 \beta_0) + u^2 (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) + \\ & + u^3 (\alpha_0 \beta_3 + \alpha_1 \beta_2 + \alpha_2 \beta_1 + \alpha_3 \beta_0) + u^4 (\alpha_0 \beta_4 + \alpha_1 \beta_3 + \alpha_2 \beta_2 + \alpha_3 \beta_1 + \alpha_4 \beta_0) + \\ & + (u^2 + 1) (\alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1) + (u^3 + u) (\alpha_2 \beta_4 + \alpha_3 \beta_3 + \alpha_4 \beta_2) + \\ & + (u^4 + u^2) (\alpha_3 \beta_4 + \alpha_4 \beta_3) + \alpha_4 \beta_4 u^8. \end{aligned}$$

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. $Q : \quad \alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4$.

$$u^5 = u^2 + 1 \Rightarrow u^6 = u^3 + u \Rightarrow u^7 = u^4 + u^2 \Rightarrow u^8 = u^3 + u^2 + 1.$$

$$\begin{aligned} & (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \\ & = \alpha_0 \beta_0 + u (\alpha_0 \beta_1 + \alpha_1 \beta_0) + u^2 (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) + \\ & + u^3 (\alpha_0 \beta_3 + \alpha_1 \beta_2 + \alpha_2 \beta_1 + \alpha_3 \beta_0) + u^4 (\alpha_0 \beta_4 + \alpha_1 \beta_3 + \alpha_2 \beta_2 + \alpha_3 \beta_1 + \alpha_4 \beta_0) + \\ & + (u^2 + 1) (\alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1) + (u^3 + u) (\alpha_2 \beta_4 + \alpha_3 \beta_3 + \alpha_4 \beta_2) + \\ & + (u^4 + u^2) (\alpha_3 \beta_4 + \alpha_4 \beta_3) + \alpha_4 \beta_4 (u^3 + u^2 + 1). \end{aligned}$$

Получим формулу для умножения в поле Q :

$$\begin{aligned} & (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \\ & = \alpha_0 \beta_0 + u (\alpha_0 \beta_1 + \alpha_1 \beta_0) + u^2 (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) + \\ & + u^3 (\alpha_0 \beta_3 + \alpha_1 \beta_2 + \alpha_2 \beta_1 + \alpha_3 \beta_0) + u^4 (\alpha_0 \beta_4 + \alpha_1 \beta_3 + \alpha_2 \beta_2 + \alpha_3 \beta_1 + \alpha_4 \beta_0) + \\ & + (u^2 + 1) (\alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1) + (u^3 + u) (\alpha_2 \beta_4 + \alpha_3 \beta_3 + \alpha_4 \beta_2) + \\ & + (u^4 + u^2) (\alpha_3 \beta_4 + \alpha_4 \beta_3) + \alpha_4 \beta_4 (u^3 + u^2 + 1) = \end{aligned}$$

Получим формулу для умножения в поле Q :

$$\begin{aligned}
 & (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \\
 & \quad = \alpha_0 \beta_0 + u (\alpha_0 \beta_1 + \alpha_1 \beta_0) + u^2 (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) + \\
 & \quad + u^3 (\alpha_0 \beta_3 + \alpha_1 \beta_2 + \alpha_2 \beta_1 + \alpha_3 \beta_0) + u^4 (\alpha_0 \beta_4 + \alpha_1 \beta_3 + \alpha_2 \beta_2 + \alpha_3 \beta_1 + \alpha_4 \beta_0) + \\
 & \quad + (u^2 + 1) (\alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1) + (u^3 + u) (\alpha_2 \beta_4 + \alpha_3 \beta_3 + \alpha_4 \beta_2) + \\
 & \quad + (u^4 + u^2) (\alpha_3 \beta_4 + \alpha_4 \beta_3) + \alpha_4 \beta_4 (u^3 + u^2 + 1) = \\
 & \quad = (\alpha_0 \beta_0 + \alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1 + \alpha_4 \beta_4) + \\
 & \quad + u (\hspace{15em}) + \\
 & + u^2 (\hspace{15em}) + \\
 & \quad + u^3 (\hspace{15em}) + \\
 & + u^4 (\hspace{15em}).
 \end{aligned}$$

Получим формулу для умножения в поле Q :

$$\begin{aligned}
& (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \\
& = \alpha_0 \beta_0 + u (\alpha_0 \beta_1 + \alpha_1 \beta_0) + u^2 (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) + \\
& + u^3 (\alpha_0 \beta_3 + \alpha_1 \beta_2 + \alpha_2 \beta_1 + \alpha_3 \beta_0) + u^4 (\alpha_0 \beta_4 + \alpha_1 \beta_3 + \alpha_2 \beta_2 + \alpha_3 \beta_1 + \alpha_4 \beta_0) + \\
& + (u^2 + 1) (\alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1) + (u^3 + u) (\alpha_2 \beta_4 + \alpha_3 \beta_3 + \alpha_4 \beta_2) + \\
& + (u^4 + u^2) (\alpha_3 \beta_4 + \alpha_4 \beta_3) + \alpha_4 \beta_4 (u^3 + u^2 + 1) = \\
& = (\alpha_0 \beta_0 + \alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1 + \alpha_4 \beta_4) + \\
& + u (\alpha_0 \beta_1 + \alpha_1 \beta_0 + \alpha_2 \beta_4 + \alpha_3 \beta_3 + \alpha_4 \beta_2) + \\
& + u^2 (\hspace{15cm}) + \\
& + u^3 (\hspace{15cm}) + \\
& + u^4 (\hspace{15cm}).
\end{aligned}$$

Получим формулу для умножения в поле Q :

$$\begin{aligned}
& (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \\
& = \alpha_0 \beta_0 + u (\alpha_0 \beta_1 + \alpha_1 \beta_0) + u^2 (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) + \\
& + u^3 (\alpha_0 \beta_3 + \alpha_1 \beta_2 + \alpha_2 \beta_1 + \alpha_3 \beta_0) + u^4 (\alpha_0 \beta_4 + \alpha_1 \beta_3 + \alpha_2 \beta_2 + \alpha_3 \beta_1 + \alpha_4 \beta_0) + \\
& + (u^2 + 1) (\alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1) + (u^3 + u) (\alpha_2 \beta_4 + \alpha_3 \beta_3 + \alpha_4 \beta_2) + \\
& + (u^4 + u^2) (\alpha_3 \beta_4 + \alpha_4 \beta_3) + \alpha_4 \beta_4 (u^3 + u^2 + 1) = \\
& = (\alpha_0 \beta_0 + \alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1 + \alpha_4 \beta_4) + \\
& + u (\alpha_0 \beta_1 + \alpha_1 \beta_0 + \alpha_2 \beta_4 + \alpha_3 \beta_3 + \alpha_4 \beta_2) + \\
& + u^2 (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0 + \alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1 + \alpha_3 \beta_4 + \alpha_4 \beta_3 + \alpha_4 \beta_4) + \\
& + u^3 (\hspace{15em}) + \\
& + u^4 (\hspace{15em}).
\end{aligned}$$

Получим формулу для умножения в поле Q :

$$\begin{aligned}
& (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \\
& = \alpha_0 \beta_0 + u (\alpha_0 \beta_1 + \alpha_1 \beta_0) + u^2 (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) + \\
& + u^3 (\alpha_0 \beta_3 + \alpha_1 \beta_2 + \alpha_2 \beta_1 + \alpha_3 \beta_0) + u^4 (\alpha_0 \beta_4 + \alpha_1 \beta_3 + \alpha_2 \beta_2 + \alpha_3 \beta_1 + \alpha_4 \beta_0) + \\
& + (u^2 + 1) (\alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1) + (u^3 + u) (\alpha_2 \beta_4 + \alpha_3 \beta_3 + \alpha_4 \beta_2) + \\
& + (u^4 + u^2) (\alpha_3 \beta_4 + \alpha_4 \beta_3) + \alpha_4 \beta_4 (u^3 + u^2 + 1) = \\
& = (\alpha_0 \beta_0 + \alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1 + \alpha_4 \beta_4) + \\
& + u (\alpha_0 \beta_1 + \alpha_1 \beta_0 + \alpha_2 \beta_4 + \alpha_3 \beta_3 + \alpha_4 \beta_2) + \\
& + u^2 (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0 + \alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1 + \alpha_3 \beta_4 + \alpha_4 \beta_3 + \alpha_4 \beta_4) + \\
& + u^3 (\alpha_0 \beta_3 + \alpha_1 \beta_2 + \alpha_2 \beta_1 + \alpha_3 \beta_0 + \alpha_2 \beta_4 + \alpha_3 \beta_3 + \alpha_4 \beta_2) + \\
& + u^4 (\hspace{15em}).
\end{aligned}$$

Получим формулу для умножения в поле Q :

$$\begin{aligned}
& (\alpha_0 + \alpha_1 u + \alpha_2 u^2 + \alpha_3 u^3 + \alpha_4 u^4) (\beta_0 + \beta_1 u + \beta_2 u^2 + \beta_3 u^3 + \beta_4 u^4) = \\
& = \alpha_0 \beta_0 + u (\alpha_0 \beta_1 + \alpha_1 \beta_0) + u^2 (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0) + \\
& + u^3 (\alpha_0 \beta_3 + \alpha_1 \beta_2 + \alpha_2 \beta_1 + \alpha_3 \beta_0) + u^4 (\alpha_0 \beta_4 + \alpha_1 \beta_3 + \alpha_2 \beta_2 + \alpha_3 \beta_1 + \alpha_4 \beta_0) + \\
& + (u^2 + 1) (\alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1) + (u^3 + u) (\alpha_2 \beta_4 + \alpha_3 \beta_3 + \alpha_4 \beta_2) + \\
& + (u^4 + u^2) (\alpha_3 \beta_4 + \alpha_4 \beta_3) + \alpha_4 \beta_4 (u^3 + u^2 + 1) = \\
& = (\alpha_0 \beta_0 + \alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1 + \alpha_4 \beta_4) + \\
& + u (\alpha_0 \beta_1 + \alpha_1 \beta_0 + \alpha_2 \beta_4 + \alpha_3 \beta_3 + \alpha_4 \beta_2) + \\
& + u^2 (\alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0 + \alpha_1 \beta_4 + \alpha_2 \beta_3 + \alpha_3 \beta_2 + \alpha_4 \beta_1 + \alpha_3 \beta_4 + \alpha_4 \beta_3 + \alpha_4 \beta_4) + \\
& + u^3 (\alpha_0 \beta_3 + \alpha_1 \beta_2 + \alpha_2 \beta_1 + \alpha_3 \beta_0 + \alpha_2 \beta_4 + \alpha_3 \beta_3 + \alpha_4 \beta_2) + \\
& + u^4 (\alpha_0 \beta_4 + \alpha_1 \beta_3 + \alpha_2 \beta_2 + \alpha_3 \beta_1 + \alpha_4 \beta_0 + \alpha_3 \beta_4 + \alpha_4 \beta_3 + \alpha_4 \beta_4).
\end{aligned}$$

Найдем все различные степени элемента u :

$$\begin{aligned}u^5 &= u^2 + 1; & u^6 &= u^3 + u; & u^7 &= u^4 + u^2; & u^8 &= u^3 + u^2 + 1; \\u^9 &= u^4 + u^3 + u; & u^{10} &= u^4 + 1; & u^{11} &= u^2 + u + 1; & u^{12} &= u^3 + u^2 + u; \\u^{13} &= u^4 + u^3 + u^2; & u^{14} &= u^4 + u^3 + u^2 + 1; & u^{15} &= u^4 + u^3 + u^2 + u + 1; \\u^{16} &= u^4 + u^3 + u + 1; & u^{17} &= u^4 + u + 1; & u^{18} &= u + 1; & u^{19} &= u^2 + u; \\u^{20} &= u^3 + u^2; & u^{21} &= u^4 + u^3; & u^{22} &= u^4 + u^2 + 1; & u^{23} &= u^3 + u^2 + u + 1; \\u^{24} &= u^4 + u^3 + u^2 + u; & u^{25} &= u^4 + u^3 + 1; & u^{26} &= u^4 + u^2 + u + 1; \\u^{27} &= u^3 + u + 1; & u^{28} &= u^4 + u^2 + u; & u^{29} &= u^3 + 1; \\u^{30} &= u^4 + u; & u^{31} &= 1.\end{aligned}$$

Для проверки, что элемент $(u + 1)$ также порождающий элемент мультипликативной группы, найдем все степени этого элемента.

Таблица 3.

n	$(u+1)^n$	n	$(u+1)^n$	n	$(u+1)^n$
2	$u^2 + 1$	12	$u^4 + u$	22	$u^4 + u^3 + u^2 + u$
3	$u^3 + u^2 + u + 1$	13	$u^4 + u + 1$	23	$u^2 + u + 1$
4	$u^4 + 1$	14	$u^2 + u$	24	$u^3 + 1$
5	$u^4 + u^2 + 1$	15	$u^2 + u$	25	$u^4 + u^3 + u + 1$
6	$u^4 + u^3 + u^2 + u + 1$	16	$u^3 + u$	26	u^3
7	u^2	17	$u^3 + u + 1$	27	$u^4 + u^3$
8	$u^3 + u^2$	18	$u^4 + u^3 + u^2 + 1$	28	$u^3 + u^2 + 1$
9	$u^4 + u^2$	19	u	29	$u^4 + u^2 + u + 1$
10	$u^4 + u^2 + u$	20	$u^2 + u$	30	$u^4 + u^3 + u^2$
11	$u^3 + u^2 + u$	21	$u^3 + u$	31	1

Пример 4. Постройте расширение \mathbb{Q} поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля \mathbb{Q} .

Решение. Найдем все подполя этого поля.

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Найдем все подполя этого поля. Его мультипликативная группа имеет порядок 31.

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Найдем все подполя этого поля. Его мультипликативная группа имеет порядок 31. Мультипликативная группа подполя является подгруппой мультипликативной группы этого поля.

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Найдем все подполя этого поля. Его мультипликативная группа имеет порядок 31. Мультипликативная группа подполя является подгруппой мультипликативной группы этого поля. Значит, по **теореме Лагранжа** порядок мультипликативной группы подполя делит нацело порядок мультипликативной группы исходного поля.

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Найдем все подполя этого поля. Его мультипликативная группа имеет порядок 31. Мультипликативная группа подполя является подгруппой мультипликативной группы этого поля. Значит, по **теореме Лагранжа** порядок мультипликативной группы подполя делит нацело порядок мультипликативной группы исходного поля. Но 31 — простое число. У него имеется только два делителя: 1 и 31.

Пример 4. Постройте расширение Q поля

$$GF(2) = \langle \{0; 1\}; \{+; \cdot; 0; 1\} \rangle$$

с помощью корня « u » многочлена $1 + x^2 + x^5$. Проверьте, что элемент $(u+1)$ является порождающим элементом мультипликативной группы этого поля. Найдите все подполя поля Q .

Решение. Найдем все подполя этого поля. Его мультипликативная группа имеет порядок 31. Мультипликативная группа подполя является подгруппой мультипликативной группы этого поля. Значит, по **теореме Лагранжа** порядок мультипликативной группы подполя делит нацело порядок мультипликативной группы исходного поля. Но 31 — простое число. У него имеется только два делителя: 1 и 31. Следовательно, поле $GF(32) = GF(2^5)$ имеет только два подполя: поле $GF(2)$ и само $GF(32)$.

Пример 5. Рассмотрим поле Q из **задачи II.5**, то есть поле, операции в котором заданы следующими таблицами Кэли:

$*$	0	e	a	b
0	0	0	0	0
e	0	e	a	b
a	0	a	b	e
b	0	b	e	a

$+$	0	e	a	b
0	0	e	a	b
e	e	0	b	a
a	a	b	0	e
b	b	a	e	0

Построить фактор-алгебру $P[x]/(P[x] * (e * x^2 + e * x + e))$.

Решение.

Пример 5. Рассмотрим поле Q из **задачи II.5**, то есть поле, операции в котором заданы следующими таблицами Кэли:

$*$	0	e	a	b
0	0	0	0	0
e	0	e	a	b
a	0	a	b	e
b	0	b	e	a

$+$	0	e	a	b
0	0	e	a	b
e	e	0	b	a
a	a	b	0	e
b	b	a	e	0

Построить фактор-алгебру $P[x]/(P[x] * (e * x^2 + e * x + e))$.

Решение. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$.

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = 0 + I = \left\{ \underbrace{0}_{g(x)=0}, \underbrace{\hspace{2cm}}_{g(x)=e}, \underbrace{\hspace{2cm}}_{g(x)=x}, \dots \right\},$$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = 0 + I = \left\{ \underbrace{0}_{g(x)=0}, \underbrace{e * x^2 + e * x + e}_{g(x)=e}, \underbrace{\hspace{10em}}_{g(x)=x}, \dots \right\},$$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = 0 + I = \left\{ \underbrace{0}_{g(x)=0}, \underbrace{e * x^2 + e * x + e}_{g(x)=e}, \underbrace{e * x^3 + e * x^2 + e * x}_{g(x)=x}, \dots \right\},$$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\},$$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\},$$

$$C_1 = e + I =$$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\},$$

$$C_1 = e + I = \{e, e * x^2 + e * x, \dots\},$$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\},$$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\},$$

$$C_2 = e * x + I =$$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\},$$

$$C_2 = e * x + I = \{e * x, e * x^2 + e, \dots\},$$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\},$$

$$C_2 = \{e * x, e * x^2 + e, \dots\},$$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\},$$

$$C_2 = \{e * x, e * x^2 + e, \dots\},$$

$$C_3 = (e * x + e) + I =$$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\},$$

$$C_3 = (e * x + e) + I = \{e * x + e, e * x^2, \dots\},$$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$\begin{aligned} C_0 &= \{0, e * x^2 + e * x + e, \dots\}, & C_1 &= \{e, e * x^2 + e * x, \dots\}, \\ C_2 &= \{e * x, e * x^2 + e, \dots\}, & C_3 &= \{e * x^2, e * x + e, \dots\}. \end{aligned}$$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$\begin{aligned} C_0 &= \{0, e * x^2 + e * x + e, \dots\}, & C_1 &= \{e, e * x^2 + e * x, \dots\}, \\ C_2 &= \{e * x, e * x^2 + e, \dots\}, & C_3 &= \{e * x^2, e * x + e, \dots\}. \end{aligned}$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$\begin{aligned} C_0 &= \{0, e * x^2 + e * x + e, \dots\}, & C_1 &= \{e, e * x^2 + e * x, \dots\}, \\ C_2 &= \{e * x, e * x^2 + e, \dots\}, & C_3 &= \{e * x^2, e * x + e, \dots\}. \end{aligned}$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(0) =$$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$\begin{aligned} C_0 &= \{0, e * x^2 + e * x + e, \dots\}, & C_1 &= \{e, e * x^2 + e * x, \dots\}, \\ C_2 &= \{e * x, e * x^2 + e, \dots\}, & C_3 &= \{e * x^2, e * x + e, \dots\}. \end{aligned}$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(0) = 0.$$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(0) = 0.$$

Поэтому

t	0
$F(t)$	0

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(x^0) =$$

Поэтому

t	$0 \quad x^0$
$F(t)$	0

.

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(x^0) = e.$$

Поэтому

t	$0 \quad x^0$
$F(t)$	0

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(x^0) = e.$$

Поэтому

t	$0 \quad x^0$
$F(t)$	$0 \quad e$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(x) =$$

Поэтому

t	$0 \quad x^0 \quad x$
$F(t)$	$0 \quad e$

.

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(x) = a.$$

Поэтому

t	$0 \quad x^0 \quad x$
$F(t)$	$0 \quad e$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\},$$

$$C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(x) = a.$$

Поэтому

t	0	x^0	x
$F(t)$	0	e	a

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(e + x) =$$

Поэтому

t	$0 \quad x^0 \quad x \quad e + x$
$F(t)$	$0 \quad e \quad a$

.

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(e + x) = e + a.$$

Поэтому

t	0	x^0	x	$e + x$
$F(t)$	0	e	a	

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(e + x) = e + a.$$

Поэтому

t	0	x^0	x	$e + x$
$F(t)$	0	e	a	$e + a$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\},$$

$$C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(x^2) =$$

Поэтому

t	0	x^0	x	$e + x$	x^2
$F(t)$	0	e	a	$e + a$	

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(x^2) = a^2 =$$

Поэтому

t	0	x^0	x	$e + x$	x^2
$F(t)$	0	e	a	$e + a$	

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(x^2) = a^2 = e + a.$$

Поэтому

t	0	x^0	x	$e + x$	x^2
$F(t)$	0	e	a	$e + a$	

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(x^2) = a^2 = e + a.$$

Поэтому

t	0	x^0	x	$e + x$	x^2
$F(t)$	0	e	a	$e + a$	$e + a$

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(e + x^2) =$$

Поэтому

t	0	x^0	x	$e + x$	x^2	$e + x^2$
$F(t)$	0	e	a	$e + a$	$e + a$	

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(e + x^2) = e + e + a =$$

Поэтому

t	0	x^0	x	$e + x$	x^2	$e + x^2$
$F(t)$	0	e	a	$e + a$	$e + a$	

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(e + x^2) = e + e + a = a.$$

Поэтому

t	0	x^0	x	$e + x$	x^2	$e + x^2$
$F(t)$	0	e	a	$e + a$	$e + a$	

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(e + x^2) = e + e + a = a.$$

Поэтому

t	0	x^0	x	$e + x$	x^2	$e + x^2$
$F(t)$	0	e	a	$e + a$	$e + a$	a

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(x + x^2) =$$

Поэтому

t	0	x^0	x	$e + x$	x^2	$e + x^2$	$x + x^2$
$F(t)$	0	e	a	$e + a$	$e + a$	a	

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(x + x^2) = a + a^2 =$$

Поэтому

t	0	x^0	x	$e + x$	x^2	$e + x^2$	$x + x^2$
$F(t)$	0	e	a	$e + a$	$e + a$	a	

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(x + x^2) = a + a^2 = a + e + a =$$

Поэтому

t	0	x^0	x	$e + x$	x^2	$e + x^2$	$x + x^2$
$F(t)$	0	e	a	$e + a$	$e + a$	a	

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(x + x^2) = a + a^2 = a + e + a = e.$$

Поэтому

t	0	x^0	x	$e + x$	x^2	$e + x^2$	$x + x^2$
$F(t)$	0	e	a	$e + a$	$e + a$	a	

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\},$$

$$C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(x + x^2) = a + a^2 = a + e + a = e.$$

Поэтому

t	0	x^0	x	$e + x$	x^2	$e + x^2$	$x + x^2$
$F(t)$	0	e	a	$e + a$	$e + a$	a	e

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(e + x + x^2) =$$

Поэтому

t	0	x^0	x	$e + x$	x^2	$e + x^2$	$x + x^2$	$e + x + x^2$
$F(t)$	0	e	a	$e + a$	$e + a$	a	e	

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольца кольца многочленов**

$$F(e + x + x^2) = e + a + a^2 =$$

Поэтому

t	0	x^0	x	$e + x$	x^2	$e + x^2$	$x + x^2$	$e + x + x^2$
$F(t)$	0	e	a	$e + a$	$e + a$	a	e	

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\},$$

$$C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(e + x + x^2) = e + a + a^2 = e + a + e + a =$$

Поэтому

t	0	x^0	x	$e + x$	x^2	$e + x^2$	$x + x^2$	$e + x + x^2$
$F(t)$	0	e	a	$e + a$	$e + a$	a	e	

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(e + x + x^2) = e + a + a^2 = e + a + e + a = 0.$$

Поэтому

t	0	x^0	x	$e + x$	x^2	$e + x^2$	$x + x^2$	$e + x + x^2$
$F(t)$	0	e	a	$e + a$	$e + a$	a	e	

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\}, \\ C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(e + x + x^2) = e + a + a^2 = e + a + e + a = 0.$$

Поэтому

t	0	x^0	x	$e + x$	x^2	$e + x^2$	$x + x^2$	$e + x + x^2$
$F(t)$	0	e	a	$e + a$	$e + a$	a	e	0

Решение примера 5. Как отмечено в решении **задачи II.5**, элемент a является корнем многочлена $f(x) = e * x^2 + e * x + e$ из $P[x]$. Следовательно, $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\}$,

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\},$$

$$C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

Из **таблиц Кэли** следует, что для функции F из доказательства **теоремы о расширении поля как фактор-кольце кольца многочленов**

$$F(e + x + x^2) = e + a + a^2 = e + a + e + a = 0.$$

Поэтому

t	0	x^0	x	$e + x$	x^2	$e + x^2$	$x + x^2$	$e + x + x^2$	\dots
$F(t)$	0	e	a	$e + a$	$e + a$	a	e	0	\dots

$$\text{Имеем } I = \left\{ g(x) \left(e * x^2 + e * x + e \right) \mid g(x) \in P[x] \right\},$$

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\},$$

$$C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

t	0	x^0	x	$e + x$	x^2	$e + x^2$	$x + x^2$	$e + x + x^2$...
$F(t)$	0	e	a	$e + a$	$e + a$	a	e	0	...

Имеем $I = \left\{ g(x) \left(e * x^2 + e * x + e \right) \mid g(x) \in P[x] \right\},$

$C_0 = \left\{ 0, e * x^2 + e * x + e, \dots \right\}, \quad C_1 = \left\{ e, e * x^2 + e * x, \dots \right\},$
 $C_2 = \left\{ e * x, e * x^2 + e, \dots \right\}, \quad C_3 = \left\{ e * x^2, e * x + e, \dots \right\}.$

t	0	x^0	x	$e + x$	x^2	$e + x^2$	$x + x^2$	e + x + x²	...
$F(t)$	0	e	a	$e + a$	$e + a$	a	e	0	...

Имеем $I = \left\{ g(x) \left(e * x^2 + e * x + e \right) \mid g(x) \in P[x] \right\},$

$$C_0 = \left\{ \mathbf{0}, \mathbf{e * x^2 + e * x + e}, \dots \right\}, \quad C_1 = \left\{ e, e * x^2 + e * x, \dots \right\},$$

$$C_2 = \left\{ e * x, e * x^2 + e, \dots \right\}, \quad C_3 = \left\{ e * x^2, e * x + e, \dots \right\}.$$

t	0	x^0	x	$e + x$	x^2	$e + x^2$	$x + x^2$	e + x + x²	...
$F(t)$	0	e	a	$e + a$	$e + a$	a	e	0	...

Имеем $I = \left\{ g(x) \left(e * x^2 + e * x + e \right) \mid g(x) \in P[x] \right\},$

$$C_0 = \left\{ 0, e * x^2 + e * x + e, \dots \right\}, \quad C_1 = \left\{ e, e * x^2 + e * x, \dots \right\},$$

$$C_2 = \left\{ e * x, e * x^2 + e, \dots \right\}, \quad C_3 = \left\{ e * x^2, e * x + e, \dots \right\}.$$

t	0	x^0	x	$e + x$	x^2	$e + x^2$	$x + x^2$	$e + x + x^2$...
$F(t)$	0	e	a	$e + a$	$e + a$	a	e	0	...

$$\text{Имеем } I = \left\{ g(x) \left(e * x^2 + e * x + e \right) \mid g(x) \in P[x] \right\},$$

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\},$$

$$C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

t	0	\mathbf{x}^0	x	$e + x$	x^2	$e + x^2$	$\mathbf{x} + \mathbf{x}^2$	$e + x + x^2$...
$F(t)$	0	\mathbf{e}	a	$e + a$	$e + a$	a	\mathbf{e}	0	...

$$\text{Имеем } I = \left\{ g(x) \left(e * x^2 + e * x + e \right) \mid g(x) \in P[x] \right\},$$

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{\mathbf{e}, \mathbf{e} * \mathbf{x}^2 + \mathbf{e} * \mathbf{x}, \dots\},$$

$$C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{e * x^2, e * x + e, \dots\}.$$

t	0	\mathbf{x}^0	x	$e + x$	x^2	$e + x^2$	$\mathbf{x} + \mathbf{x}^2$	$e + x + x^2$...
$F(t)$	0	\mathbf{e}	a	$e + a$	$e + a$	a	\mathbf{e}	0	...

Имеем $I = \left\{ g(x) \left(e * x^2 + e * x + e \right) \mid g(x) \in P[x] \right\},$

$$C_0 = \left\{ 0, e * x^2 + e * x + e, \dots \right\}, \quad C_1 = \left\{ e, e * x^2 + e * x, \dots \right\},$$

$$C_2 = \left\{ e * x, e * x^2 + e, \dots \right\}, \quad C_3 = \left\{ e * x^2, e * x + e, \dots \right\}.$$

t	0	x^0	x	$e + x$	x^2	$e + x^2$	$x + x^2$	$e + x + x^2$...
$F(t)$	0	e	a	$e + a$	$e + a$	a	e	0	...

Имеем $I = \left\{ g(x) \left(e * x^2 + e * x + e \right) \mid g(x) \in P[x] \right\},$

$$C_0 = \left\{ 0, e * x^2 + e * x + e, \dots \right\}, \quad C_1 = \left\{ e, e * x^2 + e * x, \dots \right\},$$

$$C_2 = \left\{ e * x, e * x^2 + e, \dots \right\}, \quad C_3 = \left\{ e * x^2, e * x + e, \dots \right\}.$$

t	0	x^0	x	$e + x$	x^2	e + x²	$x + x^2$	$e + x + x^2$...
$F(t)$	0	e	a	$e + a$	$e + a$	a	e	0	...

Имеем $I = \left\{ g(x) \left(e * x^2 + e * x + e \right) \mid g(x) \in P[x] \right\},$

$$C_0 = \left\{ 0, e * x^2 + e * x + e, \ldots \right\}, \quad C_1 = \left\{ e, e * x^2 + e * x, \ldots \right\},$$

$$C_2 = \left\{ \textcolor{violet}{e} * \textcolor{violet}{x}, \textcolor{violet}{e} * \textcolor{violet}{x}^2 + \textcolor{violet}{e}, \ldots \right\}, \quad C_3 = \left\{ e * x^2, e * x + e, \ldots \right\}.$$

t	0	x^0	$\textcolor{violet}{x}$	$e + x$	x^2	$\textcolor{violet}{e} + \textcolor{violet}{x}^2$	$x + x^2$	$e + x + x^2$	\ldots
$F(t)$	0	e	$\textcolor{violet}{a}$	$e + a$	$e + a$	$\textcolor{violet}{a}$	e	0	\ldots

Имеем $I = \left\{g(x) \left(e * x^2 + e * x + e \right) \mid g(x) \in P[x] \right\},$

$$C_0 = \left\{0, e * x^2 + e * x + e, \dots \right\}, \quad C_1 = \left\{e, e * x^2 + e * x, \dots \right\},$$

$$C_2 = \left\{e * x, e * x^2 + e, \dots \right\}, \quad C_3 = \left\{e * x^2, e * x + e, \dots \right\}.$$

t	0	x^0	x	$e + x$	x^2	$e + x^2$	$x + x^2$	$e + x + x^2$...
$F(t)$	0	e	a	e + a	e + a	a	e	0	...

Имеем $I = \left\{ g(x) \left(e * x^2 + e * x + e \right) \mid g(x) \in P[x] \right\},$

$$C_0 = \left\{ 0, e * x^2 + e * x + e, \ldots \right\}, \quad C_1 = \left\{ e, e * x^2 + e * x, \ldots \right\},$$

$$C_2 = \left\{ e * x, e * x^2 + e, \ldots \right\}, \quad C_3 = \left\{ e * x^2, e * x + e, \ldots \right\}.$$

t	0	x^0	x	$\mathbf{e + x}$	$\mathbf{x^2}$	$e + x^2$	$x + x^2$	$e + x + x^2$...
$F(t)$	0	e	a	$\mathbf{e + a}$	$\mathbf{e + a}$	a	e	0	...

Имеем $I = \left\{ g(x) (e * x^2 + e * x + e) \mid g(x) \in P[x] \right\},$

$$C_0 = \{0, e * x^2 + e * x + e, \dots\}, \quad C_1 = \{e, e * x^2 + e * x, \dots\},$$

$$C_2 = \{e * x, e * x^2 + e, \dots\}, \quad C_3 = \{\mathbf{e * x^2}, \mathbf{e * x + e}, \dots\}.$$

t	0	x^0	x	$\mathbf{e + x}$	$\mathbf{x^2}$	$e + x^2$	$x + x^2$	$e + x + x^2$...
$F(t)$	0	e	a	$\mathbf{e + a}$	$\mathbf{e + a}$	a	e	0	...

Вернёмся к лекции?

Задача I.1. (Ответ приведен на стр.276.) Найти таблицы Кэли операций $*$ и $+$ для простого поля $\{0, e, a\}$ характеристики 3.

Задача II.2. (Ответ приведен на стр.280.) Проверить, что многочлен $f(x) = e * x^2 + e$ неприводим над полем $P = \{0, e, a\}$ из примера I.1. Найти простое расширение поля P , соответствующее неприводимому многочлену f .

Задача II.3. (Ответ приведен на стр.296.) Проверить, является ли многочлен $f(x) = e * x^4 + a$ неприводимым над полем $P = \{0, e, a\}$. Найти простое расширение поля P , соответствующее многочлену f .

Задача II.4. (Ответ приведен на стр.304.) Проверить, является ли многочлен $f(x) = e * x^4 + a * x^3 + a * x^2 + a * x + e$ неприводимым над полем $P = \{0, e, a\}$. Найти простое расширение поля P , соответствующее многочлену f .

Задача II.5. (Ответ приведен на стр.311.) Проверить, что многочлен $f(x) = e * x^2 + e * x + e$ неприводим над полем $P = \{0, e\}$. Найти простое расширение Q поля P , соответствующее неприводимому многочлену f .

Задача II.6. (Ответ приведен на стр.319.) Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Задача III.7. (Ответ приведен на стр.337.) В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b+e)$, элемент, обратный к $(b+e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b+e)$.

Задача III.8. (Ответ приведен на стр.367.) Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Задача IV.9. (Ответ приведен на стр.394.) Для **задачи II.2** получить **таблицы Кэли** с помощью фактор-кольца кольца многочленов $P[x]$ по идеалу $I = \left\{ f(x) (e * x^2 + e) \mid f(x) \in P[x] \right\}$.

Ответы и решения

Решение задачи 1.

Задача 1. Найти таблицы Кэли операций $*$ и $+$ для простого поля $\{0, e, a\}$ характеристики 3.

Задача 1. Найти таблицы Кэли операций $*$ и $+$ для простого поля $\{0, e, a\}$ характеристики 3.

Ответ. Таблицы Кэли:

Задача 1. Найти таблицы Кэли операций $*$ и $+$ для простого поля $\{0, e, a\}$ характеристики 3.

Ответ. Таблицы Кэли:

$*$	0	e	a
0	0	0	0
e	0	e	a
a	0	a	e

Задача 1. Найти таблицы Кэли операций $*$ и $+$ для простого поля $\{0, e, a\}$ характеристики 3.

Ответ. Таблицы Кэли:

$*$	0	e	a
0	0	0	0
e	0	e	a
a	0	a	e

$+$	0	e	a
0	0	e	a
e	e	a	0
a	a	0	e

Решение задачи 2.

Задача 2. Проверить, что многочлен $f(x) = e * x^2 + e$ неприводим над полем $P = \{0, e, a\}$ из примера I.1. Найти простое расширение поля P , соответствующее неприводимому многочлену f .

Задача 2. Проверить, что многочлен $f(x) = e * x^2 + e$ неприводим над полем $P = \{0, e, a\}$ из примера I.1. Найти простое расширение поля P , соответствующее неприводимому многочлену f .

Ответ. Корней у многочлена f в поле P нет: $f(0) = e$, $f(e) = e + e = a$, $f(a) = e * a * a + e = e + e = a$.

Задача 2. Проверить, что многочлен $f(x) = e * x^2 + e$ неприводим над полем $P = \{0, e, a\}$ из примера I.1. Найти простое расширение поля P , соответствующее неприводимому многочлену f .

Ответ. Корней у многочлена f в поле P нет: $f(0) = e$, $f(e) = e + e = a$, $f(a) = e * a * a + e = e + e = a$.

Можно было рассуждать иначе: если $f(x) = 0$ для x из P , то $e * x * x = -e$, то есть $x * x = a$, но мультипликативная группа поля P имеет порядок 2, поэтому $x^2 = e$ для любого x из P .

Задача 2. Проверить, что многочлен $f(x) = e * x^2 + e$ неприводим над полем $P = \{0, e, a\}$ из примера I.1. Найти простое расширение поля P , соответствующее неприводимому многочлену f .

Ответ. Обозначим через b корень многочлена $e * x^2 + e$ в некотором расширении поля P . Характеристика поля равна 3, размерность искомого поля F , как линейного пространства над P , равна 2, в качестве базиса можно взять

Задача 2. Проверить, что многочлен $f(x) = e * x^2 + e$ неприводим над полем $P = \{0, e, a\}$ из примера I.1. Найти простое расширение поля P , соответствующее неприводимому многочлену f .

Ответ. Обозначим через b корень многочлена $e * x^2 + e$ в некотором расширении поля P . Характеристика поля равна 3, размерность искомого поля F , как линейного пространства над P , равна 2, в качестве базиса можно взять $\{e, b\}$.

Задача 2. Проверить, что многочлен $f(x) = e * x^2 + e$ неприводим над полем $P = \{0, e, a\}$ из примера I.1. Найти простое расширение поля P , соответствующее неприводимому многочлену f .

Ответ. Обозначим через b корень многочлена $e * x^2 + e$ в некотором расширении поля P . Характеристика поля равна 3, размерность искомого поля F , как линейного пространства над P , равна 2, в качестве базиса можно взять $\{e, b\}$.

Поэтому любой элемент поля F представим в виде $u * e + v * b$, где u, v принадлежат множеству $\{0, e, a\}$.

Задача 2. Проверить, что многочлен $f(x) = e * x^2 + e$ неприводим над полем $P = \{0, e, a\}$ из примера I.1. Найти простое расширение поля P , соответствующее неприводимому многочлену f .

Ответ. Обозначим через b корень многочлена $e * x^2 + e$ в некотором расширении поля P . Характеристика поля равна 3, размерность искомого поля F , как линейного пространства над P , равна 2, в качестве базиса можно взять $\{e, b\}$.

Поэтому любой элемент поля F представим в виде $u * e + v * b$, где u, v принадлежат множеству $\{0, e, a\}$.

Так как $e * b^2 + e = 0$, то $e * b^2 = -e = a$, откуда $b * b = a$.

Задача 2. Проверить, что многочлен $f(x) = e * x^2 + e$ неприводим над полем $P = \{0, e, a\}$ из примера I.1. Найти простое расширение поля P , соответствующее неприводимому многочлену f .

Ответ. Обозначим через b корень многочлена $e * x^2 + e$ в некотором расширении поля P . Характеристика поля равна 3, размерность искомого поля F , как линейного пространства над P , равна 2, в качестве базиса можно взять $\{e, b\}$.

Поэтому любой элемент поля F представим в виде $u * e + v * b$, где u, v принадлежат множеству $\{0, e, a\}$.

Имеем $b * b = a$. Сначала зададим операции формулами:

$$(\alpha + \beta * b) + (\gamma + \delta * b) =$$

Задача 2. Проверить, что многочлен $f(x) = e * x^2 + e$ неприводим над полем $P = \{0, e, a\}$ из примера I.1. Найти простое расширение поля P , соответствующее неприводимому многочлену f .

Ответ. Обозначим через b корень многочлена $e * x^2 + e$ в некотором расширении поля P . Характеристика поля равна 3, размерность искомого поля F , как линейного пространства над P , равна 2, в качестве базиса можно взять $\{e, b\}$.

Поэтому любой элемент поля F представим в виде $u * e + v * b$, где u, v принадлежат множеству $\{0, e, a\}$.

Имеем $b * b = a$. Сначала зададим операции формулами:

$$(\alpha + \beta * b) + (\gamma + \delta * b) = (\alpha + \gamma) + (\beta + \gamma) * b,$$

Задача 2. Проверить, что многочлен $f(x) = e * x^2 + e$ неприводим над полем $P = \{0, e, a\}$ из примера I.1. Найти простое расширение поля P , соответствующее неприводимому многочлену f .

Ответ. Обозначим через b корень многочлена $e * x^2 + e$ в некотором расширении поля P . Характеристика поля равна 3, размерность искомого поля F , как линейного пространства над P , равна 2, в качестве базиса можно взять $\{e, b\}$.

Поэтому любой элемент поля F представим в виде $u * e + v * b$, где u, v принадлежат множеству $\{0, e, a\}$.

Имеем $b * b = a$. Сначала зададим операции формулами:

$$(\alpha + \beta * b) + (\gamma + \delta * b) = (\alpha + \gamma) + (\beta + \gamma) * b,$$

$$(\alpha + \beta * b) * (\gamma + \delta * b) =$$

Задача 2. Проверить, что многочлен $f(x) = e * x^2 + e$ неприводим над полем $P = \{0, e, a\}$ из примера I.1. Найти простое расширение поля P , соответствующее неприводимому многочлену f .

Ответ. Обозначим через b корень многочлена $e * x^2 + e$ в некотором расширении поля P . Характеристика поля равна 3, размерность искомого поля F , как линейного пространства над P , равна 2, в качестве базиса можно взять $\{e, b\}$.

Поэтому любой элемент поля F представим в виде $u * e + v * b$, где u, v принадлежат множеству $\{0, e, a\}$.

Имеем $b * b = a$. Сначала зададим операции формулами:

$$(\alpha + \beta * b) + (\gamma + \delta * b) = (\alpha + \gamma) + (\beta + \gamma) * b,$$

$$(\alpha + \beta * b) * (\gamma + \delta * b) = \alpha * \gamma + (\alpha * \delta + \beta * \gamma) * b + \beta * \delta * b^2 =$$

Задача 2. Проверить, что многочлен $f(x) = e * x^2 + e$ неприводим над полем $P = \{0, e, a\}$ из примера I.1. Найти простое расширение поля P , соответствующее неприводимому многочлену f .

Ответ. Обозначим через b корень многочлена $e * x^2 + e$ в некотором расширении поля P . Характеристика поля равна 3, размерность искомого поля F , как линейного пространства над P , равна 2, в качестве базиса можно взять $\{e, b\}$.

Поэтому любой элемент поля F представим в виде $u * e + v * b$, где u, v принадлежат множеству $\{0, e, a\}$.

Имеем $b * b = a$. Сначала зададим операции формулами:

$$(\alpha + \beta * b) + (\gamma + \delta * b) = (\alpha + \gamma) + (\beta + \gamma) * b,$$

$$(\alpha + \beta * b) * (\gamma + \delta * b) = \alpha * \gamma + (\alpha * \delta + \beta * \gamma) * b + \beta * \delta * b^2 = (\alpha * \gamma + \beta * \delta * a) + (\alpha * \delta + \beta * \gamma) * b.$$

Задача 2. Проверить, что многочлен $f(x) = e * x^2 + e$ неприводим над полем $P = \{0, e, a\}$ из примера I.1. Найти простое расширение поля P , соответствующее неприводимому многочлену f .

Ответ. Обозначим через b корень многочлена $e * x^2 + e = 0$ в некотором расширении поля P . Характеристика поля равна 3, размерность искомого поля F , как линейного пространства над P , равна 2, в качестве базиса можно взять $\{e, b\}$.

Поэтому любой элемент поля F представим в виде $u * e + v * b$, где u, v принадлежат множеству $\{0, e, a\}$.

Имеем $b * b = a$. Зададим операции таблицами. Введем обозначения:

вектор	e	b	a	$a * b$	$e + b$	$a + b$	$e + a * b$	$a + a * b$
обозначение	e	b	a	c	d	k	m	n

Задача 2. Проверить, что многочлен $f(x) = e * x^2 + e$ неприводим над полем $P = \{0, e, a\}$ из примера I.1. Найти простое расширение поля P , соответствующее неприводимому многочлену f .

Ответ.

вектор	e	b	a	$a * b$	$e + b$	$a + b$	$e + a * b$	$a + a * b$
обозначение	e	b	a	c	d	k	m	n

Используя правила умножения многочленов (смотря на выражение $u * e + v * b$ как на многочлен от u, v , причем $b * b = a$), получим таблицу Кэли для $*$.

Например, $a * c = a * a * b = e * b = b$, $a * d = a * (e + b) = a + a * b = n$ Таким образом, с учетом

$$b^2 = a, \quad a * b^2 = a * a = e$$

имеем

Задача 2. Проверить, что многочлен $f(x) = e * x^2 + e$ неприводим над полем $P = \{0, e, a\}$ из примера I.1. Найти простое расширение поля P , соответствующее неприводимому многочлену f .

Ответ.

вектор	e	b	a	$a * b$	$e + b$	$a + b$	$e + a * b$	$a + a * b$
обозначение	e	b	a	c	d	k	m	n

Таким образом, с учетом $b^2 = a$, $2b^2 = e$ имеем

*	0	e	a	b	c	d	k	m	n
0	0	0	0	0	0	0	0	0	0
e	0	e	a	b	c	d	k	m	n
a	0	a	e	c	b	n	m	k	d
b	0	b	c	a	e	k	n	d	m
c	0	c	b	e	a	m	d	n	k
d	0	d	n	k	m	c	e	a	b
k	0	k	m	n	d	e	b	c	a
m	0	m	k	d	n	a	c	b	e
n	0	n	d	m	k	b	a	e	c

Задача 2. Проверить, что многочлен $f(x) = e * x^2 + e$ неприводим над полем $P = \{0, e, a\}$ из примера I.1. Найти простое расширение поля P , соответствующее неприводимому многочлену f .

Ответ.

вектор	e	b	a	$a * b$	$e + b$	$a + b$	$e + a * b$	$a + a * b$
обозначение	e	b	a	c	d	k	m	n

Таким образом, с учетом $b^2 = a$, $2b^2 = e$ имеем

*	0	e	a	b	c	d	k	m	n
0	0	0	0	0	0	0	0	0	0
e	0	e	a	b	c	d	k	m	n
a	0	a	e	c	b	n	m	k	d
b	0	b	c	a	e	k	n	d	m
c	0	c	b	e	a	m	d	n	k
d	0	d	n	k	m	c	e	a	b
k	0	k	m	n	d	e	b	c	a
m	0	m	k	d	n	a	c	b	e
n	0	n	d	m	k	b	a	e	c

+	0	e	a	b	c	d	k	m	n
0	0	e	a	b	c	d	k	m	n
e	e	a	0	e	k	n	b	n	c
a	a	0	e	k	n	b	d	c	m
b	b	d	k	c	0	m	n	e	a
c	c	m	n	0	b	e	a	d	k
d	d	k	b	m	e	n	c	a	0
k	k	b	d	n	a	c	m	0	e
m	m	n	c	e	d	a	0	k	b
n	n	c	m	a	k	0	e	b	d

Решение задачи 3.

Задача 3. Проверить, является ли многочлен $f(x) = e * x^4 + a$ неприводимым над полем $P = \{0, e, a\}$. Найти простое расширение поля P , соответствующее многочлену f .

Задача 3. Проверить, является ли многочлен $f(x) = e * x^4 + a$ неприводимым над полем $P = \{0, e, a\}$. Найти простое расширение поля P , соответствующее многочлену f .

Ответ. $f(a) = e + a = 0$, следовательно,

Задача 3. Проверить, является ли многочлен $f(x) = e * x^4 + a$ неприводимым над полем $P = \{0, e, a\}$. Найти простое расширение поля P , соответствующее многочлену f .

Ответ. $f(a) = e + a = 0$, следовательно, f делится на $x - a = e * x + e$:

Задача 3. Проверить, является ли многочлен $f(x) = e * x^4 + a$ неприводимым над полем $P = \{0, e, a\}$. Найти простое расширение поля P , соответствующее многочлену f .

Ответ. $f(a) = e + a = 0$, следовательно, f делится на $x - a = e * x + e$:

$$\begin{array}{r}
 e * x^4 \qquad \qquad \qquad +a \\
 e * x^4 + e * x^3 \qquad \qquad \qquad | \qquad e * x + e \\
 \hline
 a * x^3 \qquad \qquad \qquad +a \\
 a * x^3 + a * x^2 \qquad \qquad \qquad | \\
 \hline
 e * x^2 \qquad \qquad \qquad +a \\
 e * x^2 + e * x \qquad \qquad \qquad | \\
 \hline
 a * x + a \\
 a * x + a \\
 \hline
 0
 \end{array}$$

Задача 3. Проверить, является ли многочлен $f(x) = e * x^4 + a$ неприводимым над полем $P = \{0, e, a\}$. Найти простое расширение поля P , соответствующее многочлену f .

Ответ. $f(a) = e + a = 0$, следовательно, f делится на $x - a = e * x + e$:

$$\begin{array}{r}
 e * x^4 \qquad \qquad \qquad +a \\
 e * x^4 + e * x^3 \qquad \qquad \qquad \bigg| \frac{e * x + e}{e * x^3 + a * x^2 + e * x + a} \\
 \hline
 a * x^3 \qquad \qquad \qquad +a \\
 a * x^3 + a * x^2 \qquad \qquad \qquad \\
 \hline
 e * x^2 \qquad \qquad \qquad +a \\
 e * x^2 + e * x \qquad \qquad \qquad \\
 \hline
 a * x + a \\
 a * x + a \\
 \hline
 0
 \end{array}$$

$$\begin{array}{r|l} e * x^3 + a * x^2 + e * x + a & e * x + a \\ e * x^3 + a * x^2 & e * x^2 + e \\ \hline & e * x + a \\ & e * x + a \\ \hline & 0 \end{array}$$

Задача 3. Проверить, является ли многочлен $f(x) = e * x^4 + a$ неприводимым над полем $P = \{0, e, a\}$. Найти простое расширение поля P , соответствующее многочлену f .

Ответ. $f(a) = e + a = 0$, следовательно, f делится на $x - a = e * x + e$:

$$\begin{array}{r|l}
 e * x^3 + a * x^2 + e * x + a & e * x + a \\
 e * x^3 + a * x^2 & \hline
 e * x + a & \\
 e * x + a & \\
 \hline
 0 &
 \end{array}$$

Заметим, что $e * x^2 + e$ — многочлен из **примера II.2**. Итак,

$$e * x^4 + a =$$

Задача 3. Проверить, является ли многочлен $f(x) = e * x^4 + a$ неприводимым над полем $P = \{0, e, a\}$. Найти простое расширение поля P , соответствующее многочлену f .

Ответ. $f(a) = e + a = 0$, следовательно, f делится на $x - a = e * x + e$:

$$\begin{array}{r|l}
 e * x^3 + a * x^2 + e * x + a & e * x + a \\
 e * x^3 + a * x^2 & \hline
 e * x + a & \\
 e * x + a & \\
 \hline
 0 &
 \end{array}$$

Заметим, что $e * x^2 + e$ — многочлен из **примера II.2**. Итак,

$$e * x^4 + a = (x + e) * (x + a) * (e * x^2 + e),$$

Задача 3. Проверить, является ли многочлен $f(x) = e * x^4 + a$ неприводимым над полем $P = \{0, e, a\}$. Найти простое расширение поля P , соответствующее многочлену f .

Ответ. $f(a) = e + a = 0$, следовательно, f делится на $x - a = e * x + e$:

$$\begin{array}{r|l}
 e * x^3 + a * x^2 + e * x + a & e * x + a \\
 e * x^3 + a * x^2 & \hline
 e * x + a & \\
 e * x + a & \\
 \hline
 0 &
 \end{array}$$

Заметим, что $e * x^2 + e$ — многочлен из **примера II.2**. Итак,

$$e * x^4 + a = (x + e) * (x + a) * (e * x^2 + e),$$

и применяем результат **примера II.2**.

Решение задачи 4.

Задача 4. Проверить, является ли многочлен $f(x) = e * x^4 + a * x^3 + a * x^2 + a * x + e$ неприводимым над полем $P = \{0, e, a\}$.
Найти простое расширение поля P , соответствующее многочлену f .

Задача 4. Проверить, является ли многочлен $f(x) = e * x^4 + a * x^3 + a * x^2 + a * x + e$ неприводимым над полем $P = \{0, e, a\}$. Найти простое расширение поля P , соответствующее многочлену f .

Ответ. $f(a) = 0$, следовательно $f(x)$ делится на $x - a = e * x + e$. Имеем:

Задача 4. Проверить, является ли многочлен $f(x) = e * x^4 + a * x^3 + a * x^2 + a * x + e$ неприводимым над полем $P = \{0, e, a\}$. Найти простое расширение поля P , соответствующее многочлену f .

Ответ.

$$\begin{array}{r|l}
 e * x^4 + a * x^3 + a * x^2 + a * x + e & e * x + e \\
 e * x^4 + e * x^3 & \hline
 e * x^3 + a * x^2 + a * x + e & \\
 e * x^3 + e * x^2 & \hline
 e * x^2 + a * x + e & \\
 e * x^2 + e * x & \hline
 e * x + e & \\
 e * x + e & \hline
 0 &
 \end{array}$$

Задача 4. Проверить, является ли многочлен $f(x) = e * x^4 + a * x^3 + a * x^2 + a * x + e$ неприводимым над полем $P = \{0, e, a\}$. Найти простое расширение поля P , соответствующее многочлену f .

Ответ.

$$\begin{array}{r|l}
 e * x^4 + a * x^3 + a * x^2 + a * x + e & e * x + e \\
 e * x^4 + e * x^3 & \hline
 e * x^3 + a * x^2 + a * x + e & \\
 e * x^3 + e * x^2 & \hline
 e * x^2 + a * x + e & \\
 e * x^2 + e * x & \hline
 e * x + e & \\
 e * x + e & \hline
 0 &
 \end{array}$$

$$\begin{array}{r|l}
 e * x^3 + e * x^2 + e * x + e & e * x + e \\
 e * x^3 + e * x^2 & \hline
 e * x + e & \\
 e * x + e & \hline
 0 &
 \end{array}$$

Задача 4. Проверить, является ли многочлен $f(x) = e * x^4 + a * x^3 + a * x^2 + a * x + e$ неприводимым над полем $P = \{0, e, a\}$. Найти простое расширение поля P , соответствующее многочлену f .

Ответ.

$$\begin{array}{r|l}
 e * x^3 + e * x^2 + e * x + e & e * x + e \\
 e * x^3 + e * x^2 & \hline
 & e * x + e \\
 & e * x + e \\
 & \hline
 & 0
 \end{array}$$

Таким образом,

$$e * x^4 + a * x^3 + a * x^2 + a * x + e =$$

Задача 4. Проверить, является ли многочлен $f(x) = e * x^4 + a * x^3 + a * x^2 + a * x + e$ неприводимым над полем $P = \{0, e, a\}$. Найти простое расширение поля P , соответствующее многочлену f .

Ответ.

$$\begin{array}{r|l}
 e * x^3 + e * x^2 + e * x + e & e * x + e \\
 e * x^3 + e * x^2 & \hline
 e * x + e & \\
 e * x + e & \\
 \hline
 0 &
 \end{array}$$

Таким образом,

$$e * x^4 + a * x^3 + a * x^2 + a * x + e = (x + e) * (x + e) * (e * x^2 + e),$$

Задача 4. Проверить, является ли многочлен $f(x) = e * x^4 + a * x^3 + a * x^2 + a * x + e$ неприводимым над полем $P = \{0, e, a\}$. Найти простое расширение поля P , соответствующее многочлену f .

Ответ.

$$\begin{array}{r|l}
 e * x^3 + e * x^2 + e * x + e & e * x + e \\
 e * x^3 + e * x^2 & \hline
 e * x + e & \\
 e * x + e & \\
 \hline
 0 &
 \end{array}$$

Таким образом,

$$e * x^4 + a * x^3 + a * x^2 + a * x + e = (x + e) * (x + e) * (e * x^2 + e),$$

и остается применить результат **примера II.2**.

Решение задачи 5.

Задача 5. Проверить, что многочлен $f(x) = e * x^2 + e * x + e$ неприводим над полем $P = \{0, e\}$. Найти простое расширение Q поля P , соответствующее неприводимому многочлену f .

Задача 5. Проверить, что многочлен $f(x) = e * x^2 + e * x + e$ неприводим над полем $P = \{0, e\}$. Найти простое расширение Q поля P , соответствующее неприводимому многочлену f .

Ответ. Так как степень многочлена $f(x)$ равна двум, то, в силу теоремы Безу для того, чтобы убедиться в неприводимости многочлена f , достаточно проверить, что у него в поле P нет корней.

Задача 5. Проверить, что многочлен $f(x) = e * x^2 + e * x + e$ неприводим над полем $P = \{0, e\}$. Найти простое расширение Q поля P , соответствующее неприводимому многочлену f .

Ответ. Так как степень многочлена $f(x)$ равна двум, то, в силу теоремы Безу для того, чтобы убедиться в неприводимости многочлена f , достаточно проверить, что у него в поле P нет корней.

Корней действительно нет: $f(0) = e$, $f(e) = e + e + e = e$. Следовательно, f неприводим.

Задача 5. Проверить, что многочлен $f(x) = e * x^2 + e * x + e$ неприводим над полем $P = \{0, e\}$. Найти простое расширение Q поля P , соответствующее неприводимому многочлену f .

Ответ. Так как степень многочлена $f(x)$ равна двум, то, в силу теоремы Безу для того, чтобы убедиться в неприводимости многочлена f , достаточно проверить, что у него в поле P нет корней.

Корней действительно нет: $f(0) = e$, $f(e) = e + e + e = e$. Следовательно, f неприводим.

Пусть a — корень этого многочлена в некотором расширении поля P . Тогда $\{e, a\}$ — максимальная линейно независимая система векторов, поскольку $e * a * a = -e * a - e = e * a + e$ ($e = -e$, так как $e + e = 0$).

Задача 5. Проверить, что многочлен $f(x) = e * x^2 + e * x + e$ неприводим над полем $P = \{0, e\}$. Найти простое расширение Q поля P , соответствующее неприводимому многочлену f .

Ответ. В таблице сложения на диагонали стоят 0, так как характеристика поля равна 2.

Задача 5. Проверить, что многочлен $f(x) = e * x^2 + e * x + e$ неприводим над полем $P = \{0, e\}$. Найти простое расширение Q поля P , соответствующее неприводимому многочлену f .

Ответ. В таблице сложения на диагонали стоят 0, так как характеристика поля равна 2. Заметим, что в любом столбце и в любой строке каждый элемент поля встречается ровно один раз. Теперь нетрудно найти таблицы Кэли.

Задача 5. Проверить, что многочлен $f(x) = e * x^2 + e * x + e$ неприводим над полем $P = \{0, e\}$. Найти простое расширение Q поля P , соответствующее неприводимому многочлену f .

Ответ. В таблице сложения на диагонали стоят 0, так как характеристика поля равна 2. Заметим, что в любом столбце и в любой строке каждый элемент поля встречается ровно один раз. Теперь нетрудно найти таблицы Кэли.

*	0	e	a	b
0	0	0	0	0
e	0	e	a	b
a	0	a	b	e
b	0	b	e	a

Задача 5. Проверить, что многочлен $f(x) = e * x^2 + e * x + e$ неприводим над полем $P = \{0, e\}$. Найти простое расширение Q поля P , соответствующее неприводимому многочлену f .

Ответ. В таблице сложения на диагонали стоят 0, так как характеристика поля равна 2. Заметим, что в любом столбце и в любой строке каждый элемент поля встречается ровно один раз. Теперь нетрудно найти таблицы Кэли.

*	0	e	a	b
0	0	0	0	0
e	0	e	a	b
a	0	a	b	e
b	0	b	e	a

+	0	e	a	b
0	0	e	a	b
e	e	0	b	a
a	a	b	0	e
b	b	a	e	0

Решение задачи 6.

Задача 6. Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Задача 6. Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Ответ. Так как поле $GF(2) = \{0; 1\}$ имеет **характеристику** 2, то $1 + 1 = 0$, откуда $(-1) = 1$. Значит из $t^3 + t^2 + 1 = 0$ следует, что $t^3 = t^2 + 1$.

Задача 6. Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Ответ. $t^3 = t^2 + 1$,

$t^4 =$

Задача 6. Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Ответ. $t^3 = t^2 + 1$,
 $t^4 = t^3 + t =$

Задача 6. Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Ответ. $t^3 = t^2 + 1$,
 $t^4 = t^3 + t = t^2 + 1 + t$,

Задача 6. Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Ответ. $t^3 = t^2 + 1$, $t^4 = t^2 + t + 1$,
 $t^5 =$

Задача 6. Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Ответ. $t^3 = t^2 + 1$, $t^4 = t^2 + t + 1$,
 $t^5 = t^3 + t^2 + t =$

Задача 6. Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Ответ. $t^3 = t^2 + 1$, $t^4 = t^2 + t + 1$,
 $t^5 = t^3 + t^2 + t = t^2 + 1 + t^2 + t$

Задача 6. Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Ответ. $t^3 = t^2 + 1$, $t^4 = t^2 + t + 1$,
 $t^5 = t^3 + t^2 + t = t^2 + 1 + t^2 + t = t + 1$,

Задача 6. Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Ответ. $t^3 = t^2 + 1$, $t^4 = t^2 + t + 1$, $t^5 = t + 1$,
 $t^6 =$

Задача 6. Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Ответ. $t^3 = t^2 + 1$, $t^4 = t^2 + t + 1$, $t^5 = t + 1$,
 $t^6 = t^2 + t$,

Задача 6. Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Ответ. $t^3 = t^2 + 1$, $t^4 = t^2 + t + 1$, $t^5 = t + 1$, $t^6 = t^2 + t$,
 $t^7 =$

Задача 6. Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Ответ. $t^3 = t^2 + 1$, $t^4 = t^2 + t + 1$, $t^5 = t + 1$, $t^6 = t^2 + t$,
 $t^7 = t^3 + t^2 =$

Задача 6. Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Ответ. $t^3 = t^2 + 1$, $t^4 = t^2 + t + 1$, $t^5 = t + 1$, $t^6 = t^2 + t$,
 $t^7 = t^3 + t^2 = t^2 + 1 + t^2$

Задача 6. Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Ответ. $t^3 = t^2 + 1$, $t^4 = t^2 + t + 1$, $t^5 = t + 1$, $t^6 = t^2 + t$,
 $t^7 = t^3 + t^2 = t^2 + 1 + t^2 = 1$.

Задача 6. Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Ответ. $t^3 = t^2 + 1$, $t^4 = t^2 + t + 1$, $t^5 = t + 1$, $t^6 = t^2 + t$, $t^7 = 1$.

Результат согласуется с тем, что мультипликативная группа поля $GF(8)$ является циклической и ее порядок должен быть равен

Задача 6. Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Ответ. $t^3 = t^2 + 1$, $t^4 = t^2 + t + 1$, $t^5 = t + 1$, $t^6 = t^2 + t$, $t^7 = 1$.

Результат согласуется с тем, что мультипликативная группа поля $GF(8)$ является циклической и ее порядок должен быть равен $8 - 1 = 7$.

Задача 6. Найдите таблицы Кэли для расширения поля $GF(2) = \{0; 1\}$ с помощью корня t многочлена $x^3 + x^2 + 1$.

Ответ. $t^3 = t^2 + 1$, $t^4 = t^2 + t + 1$, $t^5 = t + 1$, $t^6 = t^2 + t$, $t^7 = 1$.

	+	0	1	t	$t+1$	t^2	t^2+1	t^2+t	t^2+t+1
	0	0	1	t	$t+1$	t^2	t^2+1	t^2+t	t^2+t+1
	1	1	0	$t+1$	t	t^2+1	t^2	t^2+t+1	t^2+t
	t	t	$t+1$	0	1	t^2+t	t^2+t+1	t^2	t^2+1
	$t+1$	$t+1$	t	1	0	t^2+t+1	t^2+t	t^2+1	t^2
	t^2	t^2	t^2+1	t^2+t	t^2+t+1	0	1	t	$t+1$
	t^2+1	t^2+1	t^2	t^2+t+1	t^2+t	1	0	$t+1$	t
	t^2+t	t^2+t	t^2+t+1	t^2	t^2+1	t	$t+1$	0	1
	t^2+t+1	t^2+t+1	t^2+t	t^2+1	t^2	$t+1$	t	1	0
		t^0	t^1	t^5	t^2	t^3	t^6	t^4	
	.	0	1	t	$t+1$	t^2	t^2+1	t^2+t	t^2+t+1
t^0	0	0	0	0	0	0	0	0	0
t^1	1	0	1	t	$t+1$	t^2	t^2+1	t^2+t	t^2+t+1
t^5	t	0	t	t^2	t^2+t	t^2+1	t^2+t+1	1	$t+1$
t^2	$t+1$	0	$t+1$	t^2+t	t^2+1	1	t	t^2+t+1	t^2
t^3	t^2	0	t^2	t^2+1	t^2+t+1	0	1	t	$t+1$
t^6	t^2+1	0	t^2+1	t^2+t+1	t^2+t	1	0	$t+1$	t
t^4	t^2+t	0	t^2+t	1	t^2+1	t	$t+1$	0	1
	t^2+t+1	0	t^2+t+1	$t+1$	t^2	$t+1$	t	1	0

Решение задачи 7.

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ. Мультипликативная группа расширения поля P с помощью элемента b имеет вид:

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ. Мультипликативная группа расширения поля P с помощью элемента b имеет вид:

$$Q = \{0, e, a, b, b + e, b + a, a * b, a * b + e, a * b + a\}.$$

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ. Мультипликативная группа расширения поля P с помощью элемента b имеет вид:

$$Q = \{0, e, a, b, b + e, b + a, a * b, a * b + e, a * b + a\}.$$

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \end{array} \right.$$

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ. Мультипликативная группа расширения поля P с помощью элемента b имеет вид:

$$Q = \{0, e, a, b, b + e, b + a, a * b, a * b + e, a * b + a\}.$$

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \end{array} \right.$$

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ. Мультипликативная группа расширения поля P с помощью элемента b имеет вид:

$$Q = \{0, e, a, b, b + e, b + a, a * b, a * b + e, a * b + a\}.$$

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \end{array} \right.$$

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ. Мультипликативная группа расширения поля P с помощью элемента b имеет вид:

$$Q = \{0, e, a, b, b + e, b + a, a * b, a * b + e, a * b + a\}.$$

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \end{array} \right.$$

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ. Мультипликативная группа расширения поля P с помощью элемента b имеет вид:

$$Q = \{0, e, a, b, b + e, b + a, a * b, a * b + e, a * b + a\}.$$

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \end{array} \right.$$

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ. Мультипликативная группа расширения поля P с помощью элемента b имеет вид:

$$Q = \{0, e, a, b, b + e, b + a, a * b, a * b + e, a * b + a\}.$$

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \end{array} \right.$$

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ. Мультипликативная группа расширения поля P с помощью элемента b имеет вид:

$$Q = \{0, e, a, b, b + e, b + a, a * b, a * b + e, a * b + a\}.$$

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ. Мультипликативная группа расширения поля P с помощью элемента b имеет вид:

$$Q = \{0, e, a, b, b + e, b + a, a * b, a * b + e, a * b + a\}.$$

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

В частности, обратным к $(b + e)$ является элемент $(b + e)^7 = b + a$.

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

Найдем многочлен над P , корнем которого является $(b + e)$.

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

Найдем многочлен над P , корнем которого является $(b + e)$. *Что надо найти?*

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

Найдем многочлен над P , корнем которого является $(b + e)$. *Что надо найти?*
Многочлен.

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

Найдем многочлен над P , корнем которого является $(b + e)$. *Что надо найти?*
 Многочлен. В каком виде представим ответ?

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

Найдем многочлен над P , корнем которого является $(b + e)$. *Что надо найти?* Многочлен. В каком виде представим ответ? В виде многочлена с коэффициентами из P .

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

Найдем многочлен над P , корнем которого является $(b + e)$. *Что надо найти?* Многочлен. *В каком виде представим ответ?* В виде многочлена с коэффициентами из P . *Сведем задач с значениям характеристик и введем переменные.*

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

Найдем многочлен над P , корнем которого является $(b + e)$. *Что надо найти?* Многочлен. *В каком виде представим ответ?* В виде многочлена с коэффициентами из P . *Сведем задачу с значениям характеристик и введем переменные.* Многочлен определяется своими коэффициентами.

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

Во-первых, обозначим, допустим, аргумент многочлена через x ,

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

Во-первых, обозначим, допустим, аргумент многочлена через x , во-вторых, обозначим коэффициенты многочлена буквами, допустим α (коэффициент перед x) и β (коэффициент перед x^0).

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

Итак, надо найти коэффициенты многочлена $x^2 + \alpha * x + \beta$.

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

Итак, надо найти коэффициенты многочлена $x^2 + \alpha * x + \beta$. Получим уравнение. Значение какой характеристики вычислим двумя способами?

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

Итак, надо найти коэффициенты многочлена $x^2 + \alpha * x + \beta$. Получим уравнение. Значение какой характеристики вычислим двумя способами? По условию иско-
мый многочлен обращается в ноль при $x = b + e$.

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

Итак, надо найти коэффициенты многочлена $x^2 + \alpha * x + \beta$. Получим уравнение. Значение какой характеристики вычислим двумя способами? По условию иско-мый многочлен обращается в ноль при $x = b + e$. Из этого условия и определения b получаем систему уравнений:

$$\left\{ \begin{array}{l} (b + e)^2 + \alpha * (b + e) + \beta = 0, \\ b^2 + e = 0. \end{array} \right.$$

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

$$\left\{ \begin{array}{l} (b + e)^2 + \alpha * (b + e) + \beta = 0, \\ b^2 + e = 0. \end{array} \right.$$

Из второго равенства $b^2 = a$.

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

$$\left\{ \begin{array}{l} (b + e)^2 + \alpha * (b + e) + \beta = 0, \\ b^2 + e = 0. \end{array} \right.$$

Из второго равенства $b^2 = a$. Значит, учетом $e + e = a$ и $(e + e + e) = 0$, первое уравнение системы можно преобразовать следующим образом:

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

$$\left\{ \begin{array}{l} (b + e)^2 + \alpha * (b + e) + \beta = 0, \\ b^2 + e = 0. \end{array} \right.$$

Из второго равенства $b^2 = a$. Значит, учетом $e + e = a$ и $(e + e + e) = 0$, первое уравнение системы можно преобразовать следующим образом:

$$b^2 + a * b + e + \alpha * (b + e) + \beta = 0 \Rightarrow a * b + \alpha * b + \alpha + \beta = 0 \Rightarrow b(\alpha + a) + \alpha + \beta = 0,$$

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

$$\left\{ \begin{array}{l} (b + e)^2 + \alpha * (b + e) + \beta = 0, \\ b^2 + e = 0. \end{array} \right.$$

$$b^2 + a * b + e + \alpha * (b + e) + \beta = 0 \Rightarrow a * b + \alpha * b + \alpha + \beta = 0 \Rightarrow b(\alpha + a) + \alpha + \beta = 0,$$

$$\left\{ \begin{array}{l} \alpha + a = 0, \\ \alpha + \beta = 0. \end{array} \right. \Rightarrow$$

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

$$\left\{ \begin{array}{l} (b + e)^2 + \alpha * (b + e) + \beta = 0, \\ b^2 + e = 0. \end{array} \right.$$

$$b^2 + a * b + e + \alpha * (b + e) + \beta = 0 \Rightarrow a * b + \alpha * b + \alpha + \beta = 0 \Rightarrow b(\alpha + a) + \alpha + \beta = 0,$$

$$\left\{ \begin{array}{l} \alpha + a = 0, \\ \alpha + \beta = 0. \end{array} \right. \Rightarrow \left\{ \begin{array}{l} \alpha = e, \\ \beta = a. \end{array} \right.$$

Задача 7. В примере II.2) обозначим через b корень многочлена $f(x) = e * x^2 + e$. Найдите степени элемента $(b + e)$, элемент, обратный к $(b + e)$ в мультипликативной группе соответствующего поля, и многочлен второй степени над P , корнем которого является элемент $(b + e)$.

Ответ.

$$\left\{ \begin{array}{l} (b + e)^2 = b^2 + a * b + e = a + a * b + e = a * b, \\ (b + e)^3 = a * b * (b + e) = a * a + a * b = a * b + e, \\ (b + e)^4 = (a * b + e) * (b + e) = a * b^2 + a * b + b + e = a, \\ (b + e)^5 = a * (b + e) = a * b + a = a * (b + e), \\ (b + e)^6 = a * (b + e) * (b + e) = a * a * b = b, \\ (b + e)^7 = b * (b + e) = b^2 + b = b + a, \\ (b + e)^8 = (b + a) * (b + e) = b^2 + b + b * a + a = e. \end{array} \right.$$

$$\left\{ \begin{array}{l} (b + e)^2 + \alpha * (b + e) + \beta = 0, \\ b^2 + e = 0. \end{array} \right.$$

$$b^2 + a * b + e + \alpha * (b + e) + \beta = 0 \Rightarrow a * b + \alpha * b + \alpha + \beta = 0 \Rightarrow b(\alpha + a) + \alpha + \beta = 0,$$

$$\left\{ \begin{array}{l} \alpha + a = 0, \\ \alpha + \beta = 0. \end{array} \right. \Rightarrow \left\{ \begin{array}{l} \alpha = e, \\ \beta = a. \end{array} \right.$$

Итак, искомый многочлен имеет вид $x^2 + x + a$.

Решение задачи 8.

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Применим **стратегию составления уравнений**.

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Применим **стратегию составления уравнений**. Что надо найти?

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Применим **стратегию составления уравнений**. Что надо найти?
Многочлен.

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Применим **стратегию составления уравнений**. Что надо найти?
 Многочлен. В каком виде представим ответ?

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Применим **стратегию составления уравнений**. Что надо найти? Многочлен. В каком виде представим ответ? Алгебраическим выражением.

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Применим **стратегию составления уравнений**. Что надо найти? Многочлен. В каком виде представим ответ? Алгебраическим выражением. Введем переменные.

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Применим **стратегию составления уравнений**. Что надо найти? Многочлен. В каком виде представим ответ? Алгебраическим выражением. Введем переменные. Пусть x — аргумент многочлена, и буквами обозначим коэффициенты многочлена.

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Применим **стратегию составления уравнений**. Что надо найти? Многочлен. В каком виде представим ответ? Алгебраическим выражением. Введем переменные. Пусть x — аргумент многочлена, и буквами обозначим коэффициенты многочлена. Так как $8 = 2^3$, то степень многочлена не выше 3, поэтому мы ищем многочлен $\alpha + \beta x + \gamma \cdot x^2 + x^3$.

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Применим **стратегию составления уравнений**. Что надо найти? Многочлен. В каком виде представим ответ? Алгебраическим выражением. Введем переменные. Пусть x — аргумент многочлена, и буквами обозначим коэффициенты многочлена. Так как $8 = 2^3$, то степень многочлена не выше 3, поэтому мы ищем многочлен $\alpha + \beta x + \gamma \cdot x^2 + x^3$. Составим уравнение. Значение какой величины вычислим двумя способами?

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Применим **стратегию составления уравнений**. Что надо найти? Многочлен. В каком виде представим ответ? Алгебраическим выражением. Введем переменные. Пусть x — аргумент многочлена, и буквами обозначим коэффициенты многочлена. Так как $8 = 2^3$, то степень многочлена не выше 3, поэтому мы ищем многочлен $\alpha + \beta x + \gamma \cdot x^2 + x^3$. Составим уравнение. Значение какой величины вычислим двумя способами? По условию 3 является корнем этого многочлена, т.е.

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Применим **стратегию составления уравнений**. Что надо найти? Многочлен. В каком виде представим ответ? Алгебраическим выражением. Введем переменные. Пусть x — аргумент многочлена, и буквами обозначим коэффициенты многочлена. Так как $8 = 2^3$, то степень многочлена не выше 3, поэтому мы ищем многочлен $\alpha + \beta x + \gamma \cdot x^2 + x^3$. Составим уравнение. Значение какой величины вычислим двумя способами? По условию 3 является корнем этого многочлена, т.е. $\alpha + \beta \cdot 3 + \gamma \cdot 3^2 + 3^3$.

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Применим **стратегию составления уравнений**. Что надо найти? Многочлен. В каком виде представим ответ? Алгебраическим выражением. Введем переменные. Пусть x — аргумент многочлена, и буквами обозначим коэффициенты многочлена. Так как $8 = 2^3$, то степень многочлена не выше 3, поэтому мы ищем многочлен $\alpha + \beta x + \gamma \cdot x^2 + x^3$. Составим уравнение. Значение какой величины вычислим двумя способами? По условию 3 является корнем этого многочлена, т.е. $\alpha + \beta \cdot 3 + \gamma \cdot 3^2 + 3^3$. Следовательно, $\alpha + \beta \cdot 3 + \gamma \cdot 5 + 2 = 0$.

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Осталось решить уравнение $\alpha + \beta \cdot 3 + \gamma \cdot 3^2 + 3^3$, т.е.
 $\alpha + \beta \cdot 3 + \gamma \cdot 5 + 2 = 0$.

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Осталось решить уравнение $\alpha + \beta \cdot 3 + \gamma \cdot 3^2 + 3^3$, т.е. $\alpha + \beta \cdot 3 + \gamma \cdot 5 + 2 = 0$. В данном случае, видимо, проще всего это сделать перебором, так как значения всех коэффициентов

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Осталось решить уравнение $\alpha + \beta \cdot 3 + \gamma \cdot 3^2 + 3^3$, т.е. $\alpha + \beta \cdot 3 + \gamma \cdot 5 + 2 = 0$. В данном случае, видимо, проще всего это сделать перебором, так как значения всех коэффициентов — это 0 или 1.

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Осталось решить уравнение $\alpha + \beta \cdot 3 + \gamma \cdot 3^2 + 3^3$, т.е. $\alpha + \beta \cdot 3 + \gamma \cdot 5 + 2 = 0$. В данном случае, видимо, проще всего это сделать перебором, так как значения всех коэффициентов — это 0 или 1.

$$0 + 0 \cdot 3 + 0 \cdot 5 + 2$$

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Осталось решить уравнение $\alpha + \beta \cdot 3 + \gamma \cdot 3^2 + 3^3$, т.е. $\alpha + \beta \cdot 3 + \gamma \cdot 5 + 2 = 0$. В данном случае, видимо, проще всего это сделать перебором, так как значения всех коэффициентов — это 0 или 1.

$0 + 0 \cdot 3 + 0 \cdot 5 + 2 \neq 0$,

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Осталось решить уравнение $\alpha + \beta \cdot 3 + \gamma \cdot 3^2 + 3^3$, т.е. $\alpha + \beta \cdot 3 + \gamma \cdot 5 + 2 = 0$. В данном случае, видимо, проще всего это сделать перебором, так как значения всех коэффициентов — это 0 или 1.

$0 + 0 \cdot 3 + 0 \cdot 5 + 2 \neq 0$, $1 + 0 \cdot 3 + 0 \cdot 5 + 2 =$

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Осталось решить уравнение $\alpha + \beta \cdot 3 + \gamma \cdot 3^2 + 3^3$, т.е. $\alpha + \beta \cdot 3 + \gamma \cdot 5 + 2 = 0$. В данном случае, видимо, проще всего это сделать перебором, так как значения всех коэффициентов — это 0 или 1.

$0 + 0 \cdot 3 + 0 \cdot 5 + 2 \neq 0$, $1 + 0 \cdot 3 + 0 \cdot 5 + 2 = 3 \neq 0$,

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Осталось решить уравнение $\alpha + \beta \cdot 3 + \gamma \cdot 3^2 + 3^3$, т.е. $\alpha + \beta \cdot 3 + \gamma \cdot 5 + 2 = 0$. В данном случае, видимо, проще всего это сделать перебором, так как значения всех коэффициентов — это 0 или 1.

$0 + 0 \cdot 3 + 0 \cdot 5 + 2 \neq 0$, $1 + 0 \cdot 3 + 0 \cdot 5 + 2 = 3 \neq 0$, $0 + 1 \cdot 3 + 0 \cdot 5 + 2 =$

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Осталось решить уравнение $\alpha + \beta \cdot 3 + \gamma \cdot 3^2 + 3^3$, т.е. $\alpha + \beta \cdot 3 + \gamma \cdot 5 + 2 = 0$. В данном случае, видимо, проще всего это сделать перебором, так как значения всех коэффициентов — это 0 или 1.

$0 + 0 \cdot 3 + 0 \cdot 5 + 2 \neq 0$, $1 + 0 \cdot 3 + 0 \cdot 5 + 2 = 3 \neq 0$, $0 + 1 \cdot 3 + 0 \cdot 5 + 2 = 1 \neq 0$,

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Осталось решить уравнение $\alpha + \beta \cdot 3 + \gamma \cdot 3^2 + 3^3$, т.е. $\alpha + \beta \cdot 3 + \gamma \cdot 5 + 2 = 0$. В данном случае, видимо, проще всего это сделать перебором, так как значения всех коэффициентов — это 0 или 1.

$0 + 0 \cdot 3 + 0 \cdot 5 + 2 \neq 0$, $1 + 0 \cdot 3 + 0 \cdot 5 + 2 = 3 \neq 0$, $0 + 1 \cdot 3 + 0 \cdot 5 + 2 = 1 \neq 0$,
 $1 + 1 \cdot 3 + 0 \cdot 5 + 2 =$

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Осталось решить уравнение $\alpha + \beta \cdot 3 + \gamma \cdot 3^2 + 3^3$, т.е. $\alpha + \beta \cdot 3 + \gamma \cdot 5 + 2 = 0$. В данном случае, видимо, проще всего это сделать перебором, так как значения всех коэффициентов — это 0 или 1.

$0 + 0 \cdot 3 + 0 \cdot 5 + 2 \neq 0$, $1 + 0 \cdot 3 + 0 \cdot 5 + 2 = 3 \neq 0$, $0 + 1 \cdot 3 + 0 \cdot 5 + 2 = 1 \neq 0$,
 $1 + 1 \cdot 3 + 0 \cdot 5 + 2 = 2 + 2 =$

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Осталось решить уравнение $\alpha + \beta \cdot 3 + \gamma \cdot 3^2 + 3^3$, т.е. $\alpha + \beta \cdot 3 + \gamma \cdot 5 + 2 = 0$. В данном случае, видимо, проще всего это сделать перебором, так как значения всех коэффициентов — это 0 или 1.

$0 + 0 \cdot 3 + 0 \cdot 5 + 2 \neq 0$, $1 + 0 \cdot 3 + 0 \cdot 5 + 2 = 3 \neq 0$, $0 + 1 \cdot 3 + 0 \cdot 5 + 2 = 1 \neq 0$,
 $1 + 1 \cdot 3 + 0 \cdot 5 + 2 = 2 + 2 = 0$.

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Осталось решить уравнение $\alpha + \beta \cdot 3 + \gamma \cdot 3^2 + 3^3$, т.е. $\alpha + \beta \cdot 3 + \gamma \cdot 5 + 2 = 0$. В данном случае, видимо, проще всего это сделать перебором, так как значения всех коэффициентов — это 0 или 1.

$0 + 0 \cdot 3 + 0 \cdot 5 + 2 \neq 0$, $1 + 0 \cdot 3 + 0 \cdot 5 + 2 = 3 \neq 0$, $0 + 1 \cdot 3 + 0 \cdot 5 + 2 = 1 \neq 0$,
 $1 + 1 \cdot 3 + 0 \cdot 5 + 2 = 2 + 2 = 0$.

Итак, искомым многочлен равен

Задача 8. Найдите многочлен, корнем которого является элемент 3 поля $GF(8)$, в котором полевые операции определены таблицами:

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	5	7	1	3
3	3	2	1	0	7	6	5	4	3	0	3	6	5	1	2	7	4
4	4	5	6	7	0	1	2	3	4	0	4	5	7	0	1	2	3
5	5	4	7	6	1	0	3	2	5	0	5	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1	6	0	6	1	5	2	3	0	1
7	7	6	5	4	3	2	1	0	7	0	7	3	4	3	2	1	0

Ответ. Осталось решить уравнение $\alpha + \beta \cdot 3 + \gamma \cdot 3^2 + 3^3$, т.е. $\alpha + \beta \cdot 3 + \gamma \cdot 5 + 2 = 0$. В данном случае, видимо, проще всего это сделать перебором, так как значения всех коэффициентов — это 0 или 1.

$0 + 0 \cdot 3 + 0 \cdot 5 + 2 \neq 0$, $1 + 0 \cdot 3 + 0 \cdot 5 + 2 = 3 \neq 0$, $0 + 1 \cdot 3 + 0 \cdot 5 + 2 = 1 \neq 0$,
 $1 + 1 \cdot 3 + 0 \cdot 5 + 2 = 2 + 2 = 0$.

Итак, искомый многочлен равен $1 + x + x^3$.

Решение задачи 9.

Задача 9. Для **задачи II.2** получить **таблицы Кэли** с помощью фактор-
кольца кольца многочленов $P[x]$ по идеалу $I = \left\{ f(x) (e * x^2 + e) \mid f(x) \in P[x] \right\}$.

Задача 9. Для задачи II.2 получить таблицы Кэли с помощью фактор-кольца кольца многочленов $P[x]$ по идеалу $I = \left\{ f(x) (e * x^2 + e) \mid f(x) \in P[x] \right\}$.

Ответ. Рассмотрим кольцо многочленов $P[x]$, идеал I , порожденный многочленом $f(x) = e * x^2 + e$, и фактор-кольцо $P[x]/I$. В каждом классе эквивалентных по конгруенции, соответствующей идеалу I , элементов выберем в качестве представителя многочлен минимальной степени.

Задача 9. Для **задачи II.2** получить **таблицы Кэли** с помощью фактор-кольца кольца многочленов $P[x]$ по идеалу $I = \left\{ f(x) (e * x^2 + e) \mid f(x) \in P[x] \right\}$.

Ответ. Рассмотрим кольцо многочленов $P[x]$, идеал I , порожденный многочленом $f(x) = e * x^2 + e$, и фактор-кольцо $P[x]/I$. В каждом классе эквивалентных по конгруенции, соответствующей идеалу I , элементов выберем в качестве представителя многочлен минимальной степени.

В силу теоремы о делении многочленов с остатком (алгоритм Евклида) получаем, что такими представителями являются многочлены степени

Задача 9. Для **задачи II.2** получить **таблицы Кэли** с помощью фактор-кольца кольца многочленов $P[x]$ по идеалу $I = \left\{ f(x) (e * x^2 + e) \mid f(x) \in P[x] \right\}$.

Ответ. Рассмотрим кольцо многочленов $P[x]$, идеал I , порожденный многочленом $f(x) = e * x^2 + e$, и фактор-кольцо $P[x]/I$. В каждом классе эквивалентных по конгруенции, соответствующей идеалу I , элементов выберем в качестве представителя многочлен минимальной степени.

В силу теоремы о делении многочленов с остатком (алгоритм Евклида) получаем, что такими представителями являются многочлены степени 1, так как $\deg(e * x^2 + e) = 2$.

Задача 9. Для задачи II.2 получить таблицы Кэли с помощью фактор-кольца кольца многочленов $P[x]$ по идеалу $I = \left\{ f(x) (e * x^2 + e) \mid f(x) \in P[x] \right\}$.

Ответ. Рассмотрим кольцо многочленов $P[x]$, идеал I , порожденный многочленом $f(x) = e * x^2 + e$, и фактор-кольцо $P[x]/I$. В каждом классе эквивалентных по конгруенции, соответствующей идеалу I , элементов выберем в качестве представителя многочлен минимальной степени.

В силу теоремы о делении многочленов с остатком (алгоритм Евклида) получаем, что такими представителями являются многочлены степени 1, так как $\deg(e * x^2 + e) = 2$.

Введем следующие обозначения

многочлен	e	$e * x$	$a * x$	$e + e * x$	$a + e * x$	$e + a * x$	$a + a * x$
обозначение	e	b	c	d	k	m	n

Задача 9. Для задачи II.2 получить таблицы Кэли с помощью фактор-кольца кольца многочленов $P[x]$ по идеалу $I = \left\{ f(x) (e * x^2 + e) \mid f(x) \in P[x] \right\}$.

Ответ. Рассмотрим кольцо многочленов $P[x]$, идеал I , порожденный многочленом $f(x) = e * x^2 + e$, и фактор-кольцо $P[x]/I$. В каждом классе эквивалентных по конгруенции, соответствующей идеалу I , элементов выберем в качестве представителя многочлен минимальной степени.

В силу теоремы о делении многочленов с остатком (алгоритм Евклида) получаем, что такими представителями являются многочлены степени 1, так как $\deg(e * x^2 + e) = 2$.

Введем следующие обозначения

многочлен	e	$e * x$	$a * x$	$e + e * x$	$a + e * x$	$e + a * x$	$a + a * x$
обозначение	e	b	c	d	k	m	n

Тогда, например,

Задача 9. Для задачи II.2 получить таблицы Кэли с помощью фактор-кольца кольца многочленов $P[x]$ по идеалу $I = \left\{ f(x) (e * x^2 + e) \mid f(x) \in P[x] \right\}$.

Ответ. Рассмотрим кольцо многочленов $P[x]$, идеал I , порожденный многочленом $f(x) = e * x^2 + e$, и фактор-кольцо $P[x]/I$. В каждом классе эквивалентных по конгруенции, соответствующей идеалу I , элементов выберем в качестве представителя многочлен минимальной степени.

В силу теоремы о делении многочленов с остатком (алгоритм Евклида) получаем, что такими представителями являются многочлены степени 1, так как $\deg(e * x^2 + e) = 2$.

Введем следующие обозначения

многочлен	e	$e * x$	$a * x$	$e + e * x$	$a + e * x$	$e + a * x$	$a + a * x$
обозначение	e	b	c	d	k	m	n

Тогда, например,

$$d * m =$$

Задача 9. Для задачи II.2 получить таблицы Кэли с помощью фактор-кольца кольца многочленов $P[x]$ по идеалу $I = \left\{ f(x) (e * x^2 + e) \mid f(x) \in P[x] \right\}$.

Ответ. Рассмотрим кольцо многочленов $P[x]$, идеал I , порожденный многочленом $f(x) = e * x^2 + e$, и фактор-кольцо $P[x]/I$. В каждом классе эквивалентных по конгруенции, соответствующей идеалу I , элементов выберем в качестве представителя многочлен минимальной степени.

В силу теоремы о делении многочленов с остатком (алгоритм Евклида) получаем, что такими представителями являются многочлены степени 1, так как $\deg(e * x^2 + e) = 2$.

Введем следующие обозначения

многочлен	e	$e * x$	$a * x$	$e + e * x$	$a + e * x$	$e + a * x$	$a + a * x$
обозначение	e	b	c	d	k	m	n

Тогда, например,

$$d * m = (e * e * x) * (e + a * x) =$$

Задача 9. Для задачи II.2 получить таблицы Кэли с помощью фактор-кольца кольца многочленов $P[x]$ по идеалу $I = \left\{ f(x) (e * x^2 + e) \mid f(x) \in P[x] \right\}$.

Ответ. Рассмотрим кольцо многочленов $P[x]$, идеал I , порожденный многочленом $f(x) = e * x^2 + e$, и фактор-кольцо $P[x]/I$. В каждом классе эквивалентных по конгруенции, соответствующей идеалу I , элементов выберем в качестве представителя многочлен минимальной степени.

В силу теоремы о делении многочленов с остатком (алгоритм Евклида) получаем, что такими представителями являются многочлены степени 1, так как $\deg(e * x^2 + e) = 2$.

Введем следующие обозначения

многочлен	e	$e * x$	$a * x$	$e + e * x$	$a + e * x$	$e + a * x$	$a + a * x$
обозначение	e	b	c	d	k	m	n

Тогда, например,

$$d * m = (e * e * x) * (e + a * x) = e + (a + e) * x + a * x^2 =$$

Задача 9. Для задачи II.2 получить таблицы Кэли с помощью фактор-кольца кольца многочленов $P[x]$ по идеалу $I = \left\{ f(x) (e * x^2 + e) \mid f(x) \in P[x] \right\}$.

Ответ. Рассмотрим кольцо многочленов $P[x]$, идеал I , порожденный многочленом $f(x) = e * x^2 + e$, и фактор-кольцо $P[x]/I$. В каждом классе эквивалентных по конгруенции, соответствующей идеалу I , элементов выберем в качестве представителя многочлен минимальной степени.

В силу теоремы о делении многочленов с остатком (алгоритм Евклида) получаем, что такими представителями являются многочлены степени 1, так как $\deg(e * x^2 + e) = 2$.

Введем следующие обозначения

многочлен	e	$e * x$	$a * x$	$e + e * x$	$a + e * x$	$e + a * x$	$a + a * x$
обозначение	e	b	c	d	k	m	n

Тогда, например,

$$d * m = (e * e * x) * (e + a * x) = e + (a + e) * x + a * x^2 = e + a * x^2 =$$

Задача 9. Для задачи II.2 получить таблицы Кэли с помощью фактор-кольца кольца многочленов $P[x]$ по идеалу $I = \left\{ f(x) (e * x^2 + e) \mid f(x) \in P[x] \right\}$.

Ответ. Рассмотрим кольцо многочленов $P[x]$, идеал I , порожденный многочленом $f(x) = e * x^2 + e$, и фактор-кольцо $P[x]/I$. В каждом классе эквивалентных по конгруенции, соответствующей идеалу I , элементов выберем в качестве представителя многочлен минимальной степени.

В силу теоремы о делении многочленов с остатком (алгоритм Евклида) получаем, что такими представителями являются многочлены степени 1, так как $\deg(e * x^2 + e) = 2$.

Введем следующие обозначения

многочлен	e	$e * x$	$a * x$	$e + e * x$	$a + e * x$	$e + a * x$	$a + a * x$
обозначение	e	b	c	d	k	m	n

Тогда, например,

$$d * m = (e * e * x) * (e + a * x) = e + (a + e) * x + a * x^2 = e + a * x^2 = a * (e * x^2 + e) + a.$$

Задача 9. Для задачи II.2 получить таблицы Кэли с помощью фактор-кольца кольца многочленов $P[x]$ по идеалу $I = \left\{ f(x) (e * x^2 + e) \mid f(x) \in P[x] \right\}$.

Ответ. Рассмотрим кольцо многочленов $P[x]$, идеал I , порожденный многочленом $f(x) = e * x^2 + e$, и фактор-кольцо $P[x]/I$. В каждом классе эквивалентных по конгруенции, соответствующей идеалу I , элементов выберем в качестве представителя многочлен минимальной степени.

В силу теоремы о делении многочленов с остатком (алгоритм Евклида) получаем, что такими представителями являются многочлены степени 1, так как $\deg(e * x^2 + e) = 2$.

Введем следующие обозначения

многочлен	e	$e * x$	$a * x$	$e + e * x$	$a + e * x$	$e + a * x$	$a + a * x$
обозначение	e	b	c	d	k	m	n

Тогда, например,

$$d * m = (e * e * x) * (e + a * x) = e + (a + e) * x + a * x^2 = e + a * x^2 = a * (e * x^2 + e) + a.$$

Таким образом при умножении классов, элементами которых являются d и m , то есть многочлены $e + e * x$ и $e + a * x$ соответственно, получается класс, представителем которого является многочлен a , что совпадает со значением, полученным нами ранее (см. таблицу Кэли для $*$).

Спасибо

за

внимание!

е-mail: melnikov@k66.ru, melnikov@r66.ru

сайты: <http://melnikov.k66.ru>, <http://melnikov.web.ur.ru>

[Вернуться к списку презентаций?](#)

