



Московский институт электроники и
математики им. А.Н. Тихонова

Кафедра информационной
безопасности киберфизических
систем

Москва 2024

Криптографические методы защиты информации

Поля



Понятие поля

- Кольцо F , в котором все ненулевые элементы образуют абелеву группу относительно умножения, называется **полем**.
- Кольцо F является полем тогда и только тогда, когда F есть коммутативное кольцо с единицей, в котором каждый ненулевой элемент обратим.
- Группа обратимых элементов F^* поля F состоит из всех ненулевых элементов поля F и называется мультипликативной группой данного поля.
- **Пример** поля — $(\mathbb{R}; +; \cdot)$.
- Поле, построенное на основе множества, состоящего из конечного числа элементов, называется **конечным полем**.
- **Виды** конечных полей:
 - Простые конечные поля.
 - Поля Галуа.

Простые конечные поля

- **Теорема.** Кольцо классов вычетов по модулю p является полем тогда и только тогда, когда p есть простое число.
- Кольцо классов вычетов по модулю простого числа p называется **простым конечным полем** и обозначается F_p .
- **Теорема.** Мультипликативная группа F_p^* поля F_p , где p — простое число, является циклической группой порядка $p - 1$.
- Поле F_p является полем ненулевой характеристики, $\text{char } F_p = p$.
- **Пример для $p = 7$:**
 - $F_7 = \{0, 1, 2, 3, 4, 5, 6\}$;
 - $F_7^* = \{1, 2, 3, 4, 5, 6\}$;
 - $3^2 = 2 \pmod{7}$, $3^3 = 6 \pmod{7}$,
 $3^4 = 4 \pmod{7}$, $3^5 = 5 \pmod{7}$,
 $3^6 = 1 \pmod{7}$, $\Rightarrow O(3) = 6$;
 - $F_7^* = \langle 3 \rangle = \langle 5 \rangle$.

Поля Галуа

- **Поле Галуа** назовем конечное поле F_{p^n} , полученное расширением поля F_p посредством неприводимого многочлена $f \in F_p[X]$ степени n .
- Элементами поля Галуа являются многочлены из $F_p[X]$, степень которых строго меньше n — всевозможные остатки от деления многочленов из $F_p[X]$ на неприводимый многочлен $f \in F_p[X]$.
- Мощность поля Галуа составляет p^n .
- Характеристика поля Галуа F_{p^n} совпадает с характеристикой простого конечного поля F_p : $\text{char } F_{p^n} = \text{char } F_p = p$.
- **Теорема.** Мультипликативная группа $F_{p^n}^*$ поля Галуа F_{p^n} является циклической группой порядка $p^n - 1$.



Поле Галуа – поле многочленных вычетов





Пример построения поля Галуа

- Простое конечное поле $F_3 = \{0, 1, 2\}$.
- Неприводимый многочлен $f = 2x^2 + x + 1, f \in F_3[X]$:
 - $f(0) = 1 \neq 0 \pmod{3}$;
 - $f(1) = 4 \neq 0 \pmod{3}$;
 - $f(2) = 11 \neq 0 \pmod{3}$;
- Поле Галуа $F_{3^2} = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}$.



Пример построения поля Галуа: таблица сложения

+	0	1	2	x	$x + 1$	$x + 2$	$2x$	$2x + 1$	$2x + 2$
0	0								
1	1	2							
2	2	0	1						
x	x	$x + 1$	$x + 2$	$2x$					
$x + 1$	$x + 1$	$x + 2$	x	$2x + 1$	$2x + 2$				
$x + 2$	$x + 2$	x	$x + 1$	$2x + 2$	$2x$	$2x + 1$			
$2x$	$2x$	$2x + 1$	$2x + 2$	0	1	2	x		
$2x + 1$	$2x + 1$	$2x + 2$	$2x$	1	2	0	$x + 1$	$x + 2$	
$2x + 2$	$2x + 2$	$2x$	$2x + 1$	2	0	1	$x + 2$	x	$x + 1$



Пример построения поля Галуа: таблица умножения

\cdot	1	2	x	$x + 1$	$x + 2$	$2x$	$2x + 1$	$2x + 2$
1	1							
2	2	1						
x	x	$2x$	$x + 1$					
$x + 1$	$x + 1$	$2x + 2$	$2x + 1$	2				
$x + 2$	$x + 2$	$2x + 1$	1	x	$2x + 2$			
$2x$	$2x$	x	$2x + 2$	$x + 2$	2	$x + 1$		
$2x + 1$	$2x + 1$	$x + 2$	2	$2x$	$x + 1$	1	$2x + 2$	
$2x + 2$	$2x + 2$	$x + 1$	$x + 2$	1	$2x$	$2x + 1$	x	2

Пример построения поля Галуа: исследование мультипликативной группы поля

- Найдем порядок элемента x :
 - $x^2 = x + 1, x^3 = 2x + 1, x^4 = 2, x^5 = 2x,$
 $x^6 = 2x + 2, x^7 = x + 2, x^8 = 1, \Rightarrow O(x) = 8$
- Запишем подгруппы группы $F_{3^2}^*$:
 - $F_{3^2}^* = \langle x \rangle = \langle 2x + 1 \rangle = \langle 2x \rangle = \langle x + 2 \rangle$
 - $H_1 = \langle 2 \rangle = \{1, 2\}$
 - $H_2 = \langle x + 1 \rangle = \langle 2x + 2 \rangle = \{1, x + 1, 2, 2x + 2\}$

Элемент	Степень образующего	Порядок
x	x	8
$x + 1$	x^2	4
$2x + 1$	x^3	8
2	x^4	2
$2x$	x^5	8
$2x + 2$	x^6	4
$x + 2$	x^7	8



Московский институт электроники и
математики им. А.Н. Тихонова

Кафедра информационной
безопасности киберфизических
систем

Криптографические методы
защиты информации

Спасибо за внимание!

Евсютин Олег Олегович

Заведующий кафедрой информационной безопасности киберфизических систем
Канд. техн. наук, доцент

+7 923 403 09 21

oevsyutin@hse.ru