Поля Галуа

__Поле Галуа__. Если число элементов поля конечно, то мы имеем **конечное поле**, которое также называют **полем Галуа** по имени их первого исследователя, Эвариста Галуа. Поле Галуа обозначается ***GF(q)***. Аббревиатура ***GF*** – это сокращение от словосочетания **Galois Field**, а ***q*** – число элементов поля по определению является **порядком поля**.

Определение 1. Поле Галуа *GF(q)* по определению содержит единичный элемент 1 (нейтральный элемент по умножению). Тогда, наименьшее целое число $\rho > 0$ такое, что $\underbrace{1+1+\ldots+1+1}_{\rho\ слагаемых}=0$, называют **характеристикой поля**. Отметим также, что при помощи единичного элемента поля можно породить циклическую аддитивную группу порядка ρ.

Определение 2. Пусть задан ненулевой элемент *a* поля Галуа *GF(q)*. Наименьшее целое число $\sigma > 0$ такое, что $\underbrace{a \cdot a \cdot \ldots \cdot a \cdot a}_{\sigma\ множителей} = 1$, называют **порядком элемента *a***. Отметим также, что при помощи элемента *a*, порядок которого равен σ, можно породить циклическую мультипликативную группу порядка σ.

Особо отметим, что поля Галуа существуют не для любого ***q***. Согласно общей алгебре, поле Галуа можно построить только для числа ***q***, являющегося либо простым числом ***p***, либо некоторой степенью простого числа, то есть p^m, где ***m*** – целое число ≥ 2.

Определение 3. Поле порядка *q*, являющегося простым числом *p*, называют **простым полем Галуа** и обозначают ***GF(p)***, а поле порядка $q = p^m$, называют **расширенным полем Галуа** и обозначают ***GF***(p^m), и оно является расширением простого поля *GF(p)*.

Согласно общей алгебре для заданного числа *q*, равного простому числу *p* или некоторой его степени p^m, существует одно и только одно поле Галуа *GF(q)*.

<u>Простое поле Галуа</u>. Ярким примером простого поля Галуа является поле $GF(2)$ = <{0, 1}, {+, ·}>, состоящее всего из двух элементов: 0, являющегося нейтральным элементом по сложению, и 1, являющегося нейтральным элементом по умножению, а также двух операций, сложения и умножения, со следующими «таблицами сложения и умножения»:

$GF(2)$:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Заметим, что обратным элементом по сложению для 0 является сам элемент 0, а для элемента 1 – сам элемент 1. Обратным элементом по умножению для единственного ненулевого элемента 1 – сам элемент 1. Порядок поля равен 2, поскольку поле содержит всего два элемента, кроме того, характеристика поля также равна 2, поскольку $1+1=0$, т.е. две единицы в сумме уже дают нулевой элемент.

Отметим, что простое поле $GF(2)$ является наименьшим возможным простым полем.

Приведем еще один пример простого поля $GF(3)$ = <{0, 1, 2}, {+, ·}>, с нейтральным элементом по сложению: 0, с нейтральным элементом по умножению: 1, и со следующими «таблицами сложения и умножения»:

$GF(3)$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Заметим, что обратным элементом по сложению для 0 является сам элемент 0, для 1 – элемент 2, для 2 – элемент 1. Обратным элементом по умножению элемента 1 является сам элемент 1, а для элемента 2 – сам элемент 2. Порядок поля равен 3, поскольку поле содержит всего три элемента, кроме того, характеристика поля также равна 3, поскольку $1+1+1=(1+1)+1=2+1=0$, т.е. три единицы в сумме уже дают нулевой элемент.

Наконец, приведем пример простого поля $GF(5)$ = <{0, 1, 2, 3, 4}, {+, ·}>, с нейтральным элементом по сложению: 0, с нейтральным элементом по умножению: 1, и со следующими «таблицами сложения и умножения»:

$GF(5)$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Заметим, что обратным элементом по сложению для 0 является сам элемент 0, для 1 – элемент 4, для 2 – элемент 3, для 3 – элемент 2, для 4 – элемент 1. Обратным элементом по умножению для 1 является сам элемент 1, для 2 – элемент 3, для 3 – элемент 2, для 4 – сам элемент 4. Порядок поля равен 5, поскольку оно состоит из пяти элементов. Кроме того, характеристика поля равна 5, поскольку сумма из 5 единичных элементов уже дают нулевой элемент: $1+1+1+1+1=(((1+1)+(1+1))+1)=((2+2)+1)=(4+1)=0$.