Конечные поля (поля Галуа)

В разд. 3 приведены определения математических моделей с одним классом объектов – групп, колец и полей (в частности – полей Галуа).

Можно показать, что числовое конечное поле (поле с конечным числом элементов) существует только при операциях сложения и умножения по модулю p, где p – простое число. Такие поля называются числовыми конечными полями Галуа и обозначаются $GF(p)$ или $F(p)$.

Примеры.

1. Построить конечные поля $F(2)$, $F(3)$, $F(7)$. Для решения этих примеров указать все элементы множества U, найти нейтральные и обратные элементы для групп по сложению и умножению с соответствующим модулем.

2. Показать, что не существует полей $F(6)$, $F(12)$, $F(15)$.

Поля Галуа можно построить в совершенно другой форме, а именно как поля многочленов по модулю некоторого неприводимого многочлена над числовым полем $F(p)$. В этом случае порядок поля (число его элементов) равен p^h, где p – простое, h – целое.

Пусть $F(p)$ – числовое поле Галуа порядка p. Рассмотрим множество многочленов вида

$$f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_kX^k,$$

где $a_i \in F(p)$, $i = 0, 1, 2, 3\ldots, k$, т. е. коэффициенты принимают значения из $F(p)$, операции сложения и умножения чисел выполняются по $\bmod p$. Если $a_k \neq 0$, то многочлен $f(X)$ имеет степень k. Множество всех многочленов, имеющих степень k и меньше, будем обозначать $F^{(k)}[X]$.

Введем операции сложения и умножения многочленов над полем $F(p)$ следующим образом. Пусть

$$f(X) = \sum f_iX^i \text{ и } g(X) = \sum g_iX^i.$$

Тогда

$$f(X) + g(X) = \sum_i (f_i + g_i)X^i;\ f(X)\cdot g(X) = \sum_i \left(\sum_{j=0} f_i g_{i-j} \right) X^i.$$

Например: пусть

$$f(X) = f_0 + f_1 X;\ g(X) = g_0 + g_1 X + g_2 X^2.$$

Тогда

$$f(X) + g(X) = (f_0 + g_0) + (f_1 + g_1)X + g_2 X^2;$$
$$f(X) \cdot g(X) = (f_0 g_0) + (f_0 g_1 + f_1 g_0)X + (f_1 g_1 + f_0 g_2)X^2 + f_1 g_2 X^3.$$

Отсюда видно, что при сложении степень результирующего многочлена равна максимальной степени слагаемых, а при умножении – сумме степеней перемножаемых многочленов.

Упражнения.

Сложить и перемножить следующие пары многочленов:

a) $f(X) = f_0 + f_1 X + f_2 X^2;\ g(X) = g_0 + g_1 X + g_3 X^3;$

b) $f(X) = f_1 X + f_2 X^2 + f_5 X^5;\ g(X) = g_0 + g_1 X^1 + g_4 X^4;$

c) $f(X) = f_1 X + f_2 X^2 + X^5;\ g(X) = g_0 + g_1 X^3 + g_2 X^4.$

А теперь сделайте то же самое, если указано **конечное** числовое поле (модуль):

d) $f(X) = 2X + 3X^2 + X^5;\ g(X) = 4 + 2X^3 + X^4,\ p = 7;$

e) $f(X) = 3X + 2X^2 + 2X^5;\ g(X) = 2 + 4X^1 + 3X^4,\ p = 5.$

Если рассматривать многочлены всех возможных степеней $F(X)$, то с такими операциями сложения и умножения множество многочленов образует кольцо.

Для любых двух многочленов $f(X)$ и $g(X)$ существуют, и притом единственные, многочлены $a(X)$ и $r(X)$, такие, что $f(X) = a(X)g(X) + r(X)$, где степень $g >$ степени r. Переходя к сравнениям многочленов, получаем

$$f(X) \equiv r(X) \bmod (g(X)). \qquad (6.2)$$

Деление многочленов производится так же, как и деление целых чисел. Следует только учитывать, что все операции выполняются в поле $F(p)$. Например, разделим многочлен $g(X) = 1 + X + X^2$ на $f(X) = 1 + X$ в поле $F(2)$:

$(1 + X + X^2)$	$(1 + X)$
$X + X^2$	X
1	

В результате получим $(1 + X + X^2) : (1 + X) = X$, при этом в остатке будет 1. Для деления удобнее записывать многочлены в обратном порядке, начиная со старшей степени. При вычислении в поле $F(2)$ операция сложения имеет специальное обозначение «$\oplus$» и называется «сложение по модулю 2».

Упражнения.

Найти остатки от деления многочленов:

а) $X^5 \oplus X^2 \oplus X$ на $X^3 \oplus X^2 \oplus X \oplus 1$ в поле $F(2)$ **(0)**

b) $2X^4 + X^2 + 2$ на $X^3 + 2X^2 + 2X + 1$ в поле $F(3)$ **($2X^2$)**

Если в (6.2) остаток $r(X) = 0$, то говорят, что $g(X)$ делит $f(X)$. Если в $F(X)$ нет ни одного многочлена степени, большей 0, который бы делил $f(X)$ без остатка, за исключением скалярных кратных $f(X)$, т. е. многочленов вида $bf(X)$, где $b \in F(p)$, то многочлен $f(X)$ называется *неприводимым*.

Найдем неприводимые многочлены некоторых малых степеней.

Имеется два многочлена первой степени: $X \oplus 1$ и X. По определению, они оба считаются неприводимыми.

Многочлен второй степени вида $X^2 \oplus aX \oplus b$ будет неприводимым над полем $F(2)$, если он не будет делиться ни на какой неприводимый многочлен первой степени, т. е. ни на $X \oplus 1$, ни на X. А это означает, что он не должен иметь корней в поле $F(2)$. Таким образом: $F(0) = b \neq 0$, $F(1) = 1 \oplus a \oplus b \neq 0$. Откуда получаем, что $a = 1$, $b = 1$, а сам неприводимый многочлен 2-го порядка имеет вид $X^2 \oplus X \oplus 1$.

Многочлен третьей степени имеет общий вид $X^3 \oplus aX^2 \oplus bX \oplus c$. Он будет неприводимым в поле $F(2)$, если не будет делиться ни на один из неприводимых многочленов первой степени (проверять делимость на многочлен второй степени не требуется). Таким образом, должны выполняться условия: $F(0) = c = 1$, $F(1) = 1 \oplus a \oplus b \oplus 1 = 1$. Следовательно, либо a, либо b должны равняться 1, но не оба вместе, поэтому существуют два неприводимых многочлена третьей степени: $X^3 \oplus X^2 \oplus 1$ и $X^3 \oplus X \oplus 1$.

Приведем табл. 6.1 всех неприводимых многочленов над полем $F(2)$, степень которых не превышает 4.

Возьмем один из неприводимых многочленов степени 2 над числовым полем $F(2)$, например $X^2 \oplus X \oplus 1$. При делении на этот многочлен все многочлены будут давать остатки (вычеты по модулю этого неприводимого многочлена). Приведем все виды остатков: $\{(0), (1), (X), (X \oplus 1)\}$. Каждый из этих остатков образует класс вычетов по модулю неприводимого многочлена, а их совокупность с операциями сложения и умножения по модулю неприводимого многочлена образует поле. Порядок этого поля (число элементов) в общем случае может быть равен p^h, где p – про-

Таблица 6.1

Максимальная степень многочлена	Неприводимые многочлены в поле $F(2)$
1	$X \oplus 1$; X
2	$X^2 \oplus X \oplus 1$
3	$X^3 \oplus X^2 \oplus 1$; $X^3 \oplus X \oplus 1$
4	$X^4 \oplus X^3 \oplus X^2 \oplus X \oplus 1$; $X^4 \oplus X \oplus 1$; $X^4 \oplus X^3 \oplus 1$

стое, h – целое. В приведенном примере $p = 2$, $h = 2$ и порядок поля равен 4.

Упражнение.

Постройте поля Галуа $F(2^3)$, $F(2^4)$ для пяти полиномов (многочленов), взятых из табл. 6.1.

Элемент поля α, такой, что $F(\alpha) = 0$, называется корнем многочлена $f(X)$. В этом случае говорят, что уравнение $f(X)$ имеет корень в поле $F(p)$.

Упражнения.

a) Найдите корни многочлена $X^2 + X + 1$ в полях $F(2)$, $F(3)$, $F(5)$, $F(7)$.

Покажем, как это сделать для поля $F(5)$. В уравнение

$$X^2 + X + 1 = 0 \qquad (6.3)$$

будем последовательно подставлять значения элементов поля: 0, 1, 2, 3, 4. В результате получим:

$$0^2 + 0 + 1 \equiv 1 \bmod 5;$$
$$1^2 + 1 + 1 \equiv 3 \bmod 5;$$
$$2^2 + 2 + 1 \equiv 2 \bmod 5;$$
$$3^2 + 3 + 1 \equiv 3 \bmod 5;$$
$$4^2 + 4 + 1 \equiv 1 \bmod 5,$$

т. е. этот многочлен не имеет корней в поле $F(5)$. Однако он имеет корни в поле $F(7)$. Действительно, при $X = 2$ и $X^2 = 4$ левая часть уравнения (6.3) обращается в 0.

b) Найдите корни многочлена X^4+X^3+1 в тех же полях, что и в примере 1.

Конечное поле $F(p^h)$ содержит p^h элементов. *Основное поле* $F(p)$, ко- торое является подполем поля $F(p^h)$, содержит p элементов (0, 1, 2, 3,..., $p-1$) и 2 операции: $\oplus \bmod p$ и $\otimes \bmod p$.

Элемент α называется *алгебраическим степени* h над полем $F(p)$, если и только если α удовлетворяет в $F(p)$ уравнению $P(x) = 0$, где $P(x)$ –многочлен степени h, но не удовлетворяет никакому уравнению с многочленом меньшей степени. Это влечет неприводимость многочлена $P(x)$.

Все p^h элементов поля $F(p^h)$ могут быть представлены в виде $\sum c_j \alpha^i$, где $0 \le c_j \le p-1$; $0 \le i \le h-1$. При вычислениях степень α^s, где $s \ge h$, заменяется на меньшую в соответствии с уравнением $P(\alpha) = 0$.

Пусть, например, $p = 3$, $h = 2$ и α удовлетворяет уравнению $x^2 - x - 1 = 0$. Элементы поля $F(3^2)$ можно выразить как 0, 1, 2, α, $\alpha + 1$, $\alpha + 2$, 2α, $2\alpha + 1$, $2\alpha + 2$.

В вычислениях понижение степеней производится с использованием равенства $\alpha^2 = \alpha + 1$. Например: $(2\alpha + 1)(\alpha + 2) = 2\alpha^2 + \alpha + 4\alpha + 2 = 2(\alpha + 1) + 5\alpha + 2 = 7\alpha + 4 = \alpha + 1$.

Элемент $\beta \neq 0$ поля $F(p^h)$ называется *образующей* $F^*(p^h)$ мультипликативной группы ненулевых элементов поля $F(p^h)$, если степени β^i, $i = 1, 2, 3, \ldots, p^h - 1$ пробегают все ненулевые элементы поля $F(p^h)$. Образующая может рассматриваться как основание log. Такие логарифмы называются *дискретными логарифмами*. Рассмотрим, например, все 8 степеней (кроме нулевой) корня α в приведенном выше примере и запишем результат в виде таблицы:

i	1	2	3	4	5	6	7	8
α^i	α	$\alpha + 1$	$2\alpha + 1$	2	2α	$2\alpha + 2$	$\alpha + 2$	1

Из таблицы видно, что α является образующей. Эта таблица может быть представлена как таблица дискретных логарифмов. Для этого в верхней строке запишем упорядоченные элементы поля, а в нижней – значения степеней образующего элемента, при которых получаем данный элемент поля:

y	1	2	α	$\alpha + 1$	$\alpha + 2$	2α	$2\alpha + 1$	$2\alpha + 2$
$\log_\alpha y$	8	4	1	2	7	5	3	6

Считается, что вычисление дискретных логарифмов является трудной задачей, как и задача факторизации (разложения на множители), что является существенным в криптосистемах с открытым распределением ключей. Таблица логарифмов может использоваться для выполнения умножения и деления элементов поля. Заметим, что операции выполняются по модулю $p^h - 1$, в данном примере – по модулю $3^2 - 1 = 8$.

Для примера: $\log((\alpha + 2)(2\alpha + 1)) = \log(\alpha + 2) + \log(2\alpha + 1) = 7 + 3 = 10 \equiv 2 \bmod 8$. Что соответствует элементу $\alpha + 1$. $\log((\alpha + 1)/(2\alpha + 2)) = 2 - 6 = -4 \equiv 4 \bmod 8$, что соответствует элементу 2.

Можно проверить, что кроме элемента α образующими β также являются элементы $2\alpha + 1$, $\alpha + 2$ и 2α. Если $s = p^h - 1$ есть наименьшая положительная степень, удовлетворяющая уравнению $\beta^s = 1$, то β является образующей. Поэтому число образующих элементов поля равно $\varphi(p^h - 1)$, где φ – функция Эйлера. Для нашего примера $\varphi(8) = 4$.

Упражнения.

Найдите количество образующих элементов для полей Галуа: $F(3^4)$, $F(5^2)$, $F(7^2)$, $F(11^5)$, $F(13^4)$.

Рассмотрим поле Галуа $F(p^h)$ при $p > 2$ и h – целом. Исключим из элементов поля нулевой элемент, а оставшееся множество обозначим $F^*(p^h)$.