Защита информации

Павел Юдаев

МГТУ им. Баумана, Кафедра ИУ-9

Москва, 2014

Раздел 11 - Конечные поля

Конечные поля

Опр.

Пусть G - непустое множество, $*$ - бинарная операция, определенная $\forall a, b \in G$. $(G, *)$ - *группа*, если:

- $\forall a, b \in G \; a * b \in G$ (замкн.)
- $\forall a, b, c \in G \; (a * b) * c = a * (b * c)$ (ассоц.)
- $\exists e \in G : \forall a \in G \; a * e = e * a = a$ (сущ. нейтр.эл.)
- $\forall a \in G \;\; \exists a^{-1} \in G : a * a^{-1} = a^{-1} * a = e$ (сущ. обратного эл.)

Опр.

Абелева (коммутативная) группа: $a * b = b * a$

Опр.

Порядок группы $(G, *)$ - мощность G, обозн. $|G|$

Опр.

Возведение в степень: $a \in G, i \in N \;\; a^i = (a * ... * a)$ i раз.
$a^0 = 1$ (1 - это e)

Опр.

Порядок элемента $a \in G$ - это $min\ n \neq 0 : \;\; a^n = 1$.

Опр.

Подгруппа группы G - подмножество G, которое является группой относительно $*$.

Опр.

Смежный класс множества H по элементу a - это
$aH = \{ax | x \in H\}$

Пример

$\mathbb{Z}_{10}^{+}$ - группа. Пример подгруппы и смежных классов.

Теорема 1 (Т. Лагранжа)

Пусть H - подгруппа G. Тогда
$|G| = |H| * (\text{количество смежных классов по } H)$

Без док-ва.

Пример

- Группа вычетов по модулю N по сложению: $\mathbb{Z}_N = \{0, 1, ..N-1\}$
- Группа по умножению на $\mathbb{Z}_N$: $\mathbb{Z}_N^* = \{i \in \mathbb{Z}_N | \text{НОД}(i, N) = 1\}$

Утверждение

Группа по умножению на $\mathbb{Z}_N$: $\mathbb{Z}_N^* = \{i \in \mathbb{Z}_N | \text{НОД}(i, N) = 1\}$

Доказать.

Следствие: если G - группа конечного порядка k, то порядок k_1 любой ее подгруппы G_1 является делителем порядка группы.

Опр.

Группа наз. *циклической*, если
$\exists a \in G : \ \forall b \in G \ \exists i \in N : \ b = a^i$. a наз. *генератором* (*порождающим элементом*) группы. Обозн. $G = < a >$.

Следствие: порядок любого элемента - делитель порядка группы.

Следствие: Пусть $m = |G|$. Тогда $\forall a \in G \ a^m = 1$

Задача

$5^{38} \ mod \ 9 \ = ?$
$3^{663} mod \ 7 \ = ?$

Опр.

Кольцо $(R, +, *)$ (или просто R):

- R - абелева группа по $+$
- $\forall a, b \in G\ a * b \in G$ (замкн. *)
- $\forall a, b, c \in G\ (a * b) * c = a * (b * c)$ (ассоц. *)
- $\forall a, b, c \in G\ a(b + c) = ab + ac$ и $(b + c)a = ba + ca$ (дистр. справа и слева)

Если * комм., то это коммутативное кольцо.

Опр.

Делители нуля: если $a * b = 0$ в кольце.

Опр.

Поле $(F, +, *)$ (или просто F):

- $(F, +, *)$ - кольцо
- $(F \setminus \{0\}, *)$ - абелева группа

Нейтральный элемент по + обозн. 0.

Нейтральный элемент по * обозн. 1.

Поле - коммутативное кольцо с $1 \neq 0$ без делителей нуля.

Опр.

Характеристика поля - $min\ n \in \mathbb{N}$ такое, что сумма n копий единицы равна нулю: $n \cdot 1 = 0$ Если такого числа не существует, то характеристика равна 0.

Опр.

$H \subseteq F$ - подполе поля $(F, +, *)$, если H замкнуто отн. $+$, *.

Опр.

$H \supset F$ - расширение поля F, если H - поле и F - подполе H.

Опр.

Поле Галуа - конечное поле. Обозн. $GF(q)$, q - порядок поля. (Эварист Галуа, 1811 - 1832).

Опр.

Простое поле - поле, не содержащее собственных подполей.

Свойства поля:

- Характеристика конечного поля - простое число.
  Док. от противного.
- Пусть F - конечное поле, k - его порядок. Тогда $k = p^n$, p - простое, $n \in N$. Причем p - характеристика поля.
  Без док-ва.
- Для любого p^n (p - простое) существует единственное (с точностью до изоморфизма) поле порядка p^n, обозн. F_{p^n}.
  Без док-ва.
- Мультипликативная группа F_q^* поля F_q - циклическая группа порядка $(q-1)$. Ее генератор наз. *примитивным элементом* поля.
  Без док-ва.

Пример (Не циклическая группа)

$\mathbb{Z}_8^* = (\{1, 3, 5, 7\}, *)$.

$|G| = 4$. $g_i^2 = e$.

Пример (Циклическая группа)

$\mathbb{Z}_7^*$

Пример (Поле)

GF(2), {0,1}, + это XOR, * это AND.

TODO: здесь надо остановиться!
Дальнейший материал про расширения полей имеет смысл, только если подробно рассказывать AES
(это не нужно делать!)
или если успеть в конце дойти до теории кодирования (я за один семестр не успеваю).

Обозн.: $F_p[x]$ - кольцо полиномов не ограниченной степени с коэффициентами из поля F_p.
$a_n * x^n + ... + a_0, \quad a_i \in F_p, \;\; x$ - формальный символ.

$f(x) \cdot g(x)$ в $F_p[x]$: как обычно:
степени x складываются в кольце $\mathbb{Z}$;
операции над коэффициентами - из F_p.

Деление полиномов с остатком: "в столбик"
($GF(2)[x]$, $x^3 + x + 1$ на $x + 1$)

Опр.

Неприводимый многочлен - не имеет делителей в $F_p[x]$, т.е. не разлагается в произведение других многочленов.

$x^4 + x^2 + 1 = (x^2 + 1)(x^2 + 1)$ не имеет корней.

Корни многочленов

$q = p^n$

$\forall a \in GF(q)$ одночлен $x - a$ имеет корень a.

Рассмотрим многочлен $f(x) = x^q - x$ над $GF(q)$. По основной теореме алгебры, полином степени q имеет не более q корней.

В поле нет делителей нуля, поэтому $|GF^*(q)| = q - 1$.
$\Rightarrow \forall a \in GF^*(q)\ a^{q-1} = 1$.

$\Rightarrow f(x)$ имеет q различных корней, т.е. $f(x) = \prod\limits_{a \in GF(q)} (x - a)$.

Построим расширение конечного поля.

Опр.

Идеал кольца R - подкольцо $I \subset R$:
$\forall i \in I \ \forall r \in R \ \ ir \in I$ (правый идеал).

Опр.

Изоморфизм - биекция, сохраняющая операции.

Пример

- $\{5k | k \in \mathbb{Z}\} = < 5 >$ - подкольцо $\mathbb{Z}$, идеал.
  Факторкольцо $Z/ < 5 > \cong (\mathbb{Z}_5, +, *)$ - поле.
- $\{6k | k \in \mathbb{Z}\} = < 6 >$ - подкольцо $\mathbb{Z}$, идеал.
  Факторкольцо $Z/ < 6 > \cong (\mathbb{Z}_6, +, *)$ - кольцо.

Опр.

Пусть $GF(p)[x]$ - кольцо многочленов. *Расширение поля* $GF(p)$ - это *факторкольцо* $R(p^n)$ - кольцо классов вычетов $GF(p)[x]$ по модулю его идеала.

$$R(p^n) = GF(p)[x] / < f_n(x) >,$$

где $f_n(x)$ - многочлен степени n над $GF(p)$,
и $< f_n(x) >$ - подкольцо всех мночленов, кратных $f_n(x)$.

Утверждение

Если $f_n(x)$ - неприводимый многочлен, то
$GF(p^n) = \overline{GF(p)[x]/ < f_n(x) >}$ - поле, расширение поля $GF(p)$.
(Проверим, что аксиомы поля вып-ся.)

В $F[x]/ < g >$ все операции над полиномами - по модулю g. Так же, как в $\mathbb{Z}_n = \mathbb{Z}/ < n >$ все операции - по модулю n.

Пример (Для семинара)

1) $f(x) = x^2 + 1$. Построить $F_2/ < f(x) >$. Найти делители нуля.

2) $f(x) = x^2 + x + 1$. Построить $F_2/ < f(x) >$. Показать, что это поле. (См. слайд 24.)

F_p - поле, p - простое.

Пусть $F = F_p[x]/ < g >$, где

$g = g_n(x) = \sum_{i=0}^{n} a_i x^i \in F_p[x]$ - неприводимый над полем F_p.

Тогда для элемента $[x] \in F$ верно

$g([x]) = \sum_{i=0}^{n} a_i([x]^i) = \left[\sum_{i=0}^{n} a_i(x^i) \right] = [g] = [0]$ в F.

Т.е. элемент $\alpha = [x] \in F$ - корень многочлена $g(x)$ в поле F.

$g_n(x)$ - неприводимый. $F_q = F_p[x]/ < g >$.

1) $\alpha = [x] \in F$ - корень $g(x)$ в F_q

2) F_q^* - циклическая. $\exists$ генератор (образующий элемент) $\beta \in F_q \setminus \{0\}$. Порядок $\beta = |F_q^*|$.

$\alpha =? \beta$

Опр.

Неприводимый многочлен $g(x)$ является *примитивным*, если его корень $\alpha = [x]$ - генератор (образующий элемент) мультипликативной группы поля $F_q = F_p[x]/ < g >$.

Следствие: все элементы $F_p[x]/ < g >$ - корни примитивного $g(x)$.

Пример (Для семинара)

Неприводимый $g(x) = x^4 + x + 1$. $F = GF(16) = F_2/g(x)$.

$\alpha = x \in F$ - корень $g(x)$.

α - генератор поля?
$|F^*| = 15$. Проверим $\alpha^3 = x^3 \neq 1$.
$\alpha^5 = \alpha^4 \cdot \alpha = (\alpha + 1)\alpha = (x + 1)x \neq 1$
Значит $ord(\alpha) = 15$, α - генератор F.

Пример (Для семинара)

Неприводимый $g(x) = x^4 + x^3 + x^2 + x + 1$.
$H = GF(16) = F_2/ < g(x) >$. $H \cong F$.

$\alpha = x \in H$ - корень $g(x)$.

α - генератор поля?
$|H^*| = 15$. Проверим $\alpha^3 = x^3 \neq 1$.
$\alpha^5 = \alpha^4 \cdot \alpha = (\alpha^3 + \alpha^2 + \alpha + 1)\alpha = 1$
Т.к. $(x^3 + x^2 + x + 1)x = 1 \; \forall \gamma \in H$
Значит $ord(\alpha) = 5$, α - не генератор F.

Сущ. другой генератор F - не корень $g(x)$.

Поле как векторное линейное пространство

$\forall \gamma \in F_p / < g_n(x) > \ \gamma = b_{n-1}\alpha^{n-1} + ... + b_1\alpha + b_0$

где $b_i \in F_p \ \forall i$.

$\gamma \in F_{p^n} \leftrightarrow (b_{n-1}, .., b_1, b_0)$

- Операция сложения элементов поля $F_p / < g_n(x) >$ - это операция покоординатного сложения задающих их векторов.
- Абелева группа по $+$
- Умножение на скаляр - элемент F_p - ассоциативное, дистрибутивное.

Размерность лин. пр-ва равна $n = deg(g)$.

$\gamma \in F_{p^n} \leftrightarrow (b_{n-1}, .., b_1, b_0)$, где $b_i \in F_p$.

Например, элементы $GF(2)/ < x^4 + x + 1 > = GF(16)$:
(1011) кодирует $x^3 + x + 1$ и т.д.

Все 8-битные последовательности (байты) кодируют элементы поля $GF(256) = GF(2)[x]/ < g_8(x) >$, $deg(g_8) = 8$.

Опр.

Дискретный логарифм $log_a b = x$, где $a, b \in F$, $x \in \mathbb{Z}$ - это $x : a^x = b$.

$log\ b = log_\alpha b$, где α - примитивный элемент поля.

$F_2/ < x^2 + x + 1 >= GF(4)$:

Последовательность длины 2	Многочлен	Степень	Логарифм
00	0	0	$-\infty$
01	1	1	0
10	x	α	1
11	x + 1	α^2	2

Расширение поля $GF(2)$ по модулю многочлена $\pi(x) = x^2 + x + 1$.

Правила сложения и умножения в этом поле

+	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

Сложение в поле $GF(4)$ по модулю $\pi(x) = x^2 + x + 1$.

•	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

Умножение в поле $GF(4)$ по модулю $\pi(x) = x^2 + x + 1$.

Замеч.: при построении расширения поля $GF(q)$ само поле $GF(q)$ может быть расширением некоторого поля, т.е. возможно $q = (p^m)^k$, p - простое.

Задача

Сколькими способами можно построить $GF(n)$, $n = 8, 9, 16, 18$?

Литература к лекции

1. Лидл, Нидеррайтер. *Конечные поля*. Том 1, глава 1.

2. А.А.Болотов, С.Б.Гашков, А.Б.Фролов, А.А.Часовских. *Алгоритмические основы эллиптической криптографии*, глава 1.

3*. V. Shoup, *A Computational Introduction to Number Theory and Algebra*, 2008