Домашнее задание 6

Ешмуратов Айбат

Июль 2022

Аннотация

Разбор домашнего задания по Алгебре по темам конечные поля, мультипликативные группы, приводимость многочленов и подполья.

Оглавление

Часть I

Домашнее задание

Глава 1

Разбор

1.1 Операции в полях

- Таблица аддитивной и мультипликативной инверсий

	0	1	2	3	4
Аддитивная инверсия	0	4	3	2	1
Мультипликативная инверсия	–	1	2	3	4

- Пример поля на множестве Z_5 с операцией умножения.

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Вот некоторые определения и иллюстрации, которые пригодятся для выполнения заданий.

Рис. 1.1: Пример аддитивной инверсии

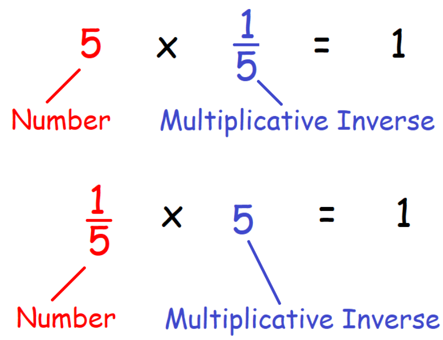

Рис. 1.2: Пример мультипликативной инверсии

- Пусть K – поле [1] $\rightarrow R = K[x_1, \ldots, x_n]$ – кольцо многочленов от переменных $x_1, \ldots, x_n$

- Старшим членом многочлена $f \in R \setminus \{0\}$ называется наибольший в лексикографическом порядке одночлен из $M(f)$.
- Многочлен g редуцируется к $g^{'}$ через систему F, если существует цепочка элементарных редукций $g \xrightarrow{f_1} g_1 \xrightarrow{f_2} g_2 \xrightarrow{f_3} \ldots \xrightarrow{f_k} g_k = g^{'},\ f_i \in F$.
- Многочлен $S(f_1, f_2) = k_1 f_2 - k_2 f_2$ называется *S-многочленом* многочленов f_1 и f_2.
- $S(f_1, f_2) = -S(f_1, f_2)$

1.2 Задание 1

Какие значения может принимать длина убывающей (в лексикографическом порядке) цепочки одночленов от переменных x_1, x_2, x_3, начинающейся с одночлена $x_1x_2^3x_3^2$ и заканчивающейся одночленом $x_1x_2^2x_3^3$?

1. Цепочка может быть длины ≥ 2, в силу того, что в условии даны как минимум два одночлена цепочки. Построим цепь в лексикографическом порядке, чтобы узнать какие значения может принимать длина цепочки.

$$x_1x_2^3x_3^2 > x_1x_2^2x_3^3 \tag{1.1}$$

2. При n $\geq$ 4 верно следующее

$$x_1x_2^3x_3^2 > x_1x_2^2x_3^n > x_1x_2^2x_3^{n-1} > ...... > x_1x_2^2x_3^3 \tag{1.2}$$

3. Получаем, что в этой цепочке n одночленов, где одночленов $x_1x_2^2x_3^i$ n - 1 штук. Значит цепочка может принимать значения n $\geq$ 2, n $\in$ N.

Ответ: n $\geq$ 2, n $\in$ N

Лексикографический порядок может быть применим в поразрядной сортировке.

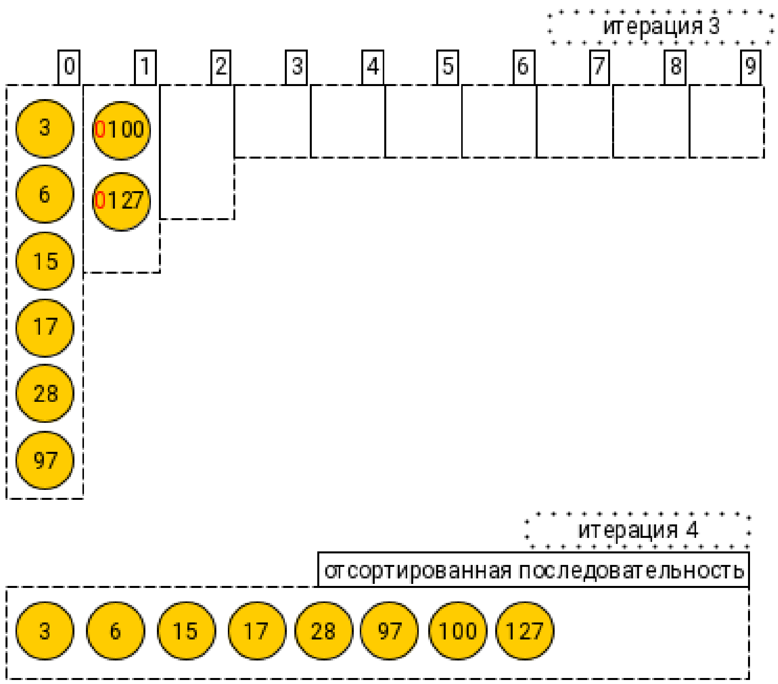

Рис. 1.3: Поразрядная сортировка

1.3 Задание 2

Найдите остаток многочлена g относительно системы $\{f\}$, где

$$g = x_2^4x_3^5 + 2x_1x_2^4x_3 + x_1^2x_2^2 \qquad f = x_2^4x_3 - 2x_1x_2x_3^2 + x_1x_2^2$$

Чтобы найти остаток проделаем элементарные редукции [3].

$$x_1^4x_5^2 + 2x_1x_2^4x_3 + x_1^2x_2^2 - (f \cdot x_1) = x_1x_2^4x_3 + x_2^4x_3^5 + 2x_1^2x_2x_3^2 \tag{1.3}$$

$$x_1x_2^4x_3 + x_2^4x_3^5 + 2x_1^2x_2x_3^2 - (f \cdot x_2^2x_3) = 2x_1^2x_2x_3^2 + 2x_1x_2^3x_3^3 - x_2^6x_3^2 + x_2^4x_5 \tag{1.4}$$

$$2x_1^2x_2x_3^2 + 2x_1x_2^3x_3^3 - x_2^6x_3^2 + x_2^4x_5 - (f \cdot 2x_2x_3^3) = 2x_1^2x_2x_3^2 + x_2^4x_3^5 - x_2^6x_3^2 + 4x_1x_2^2x_3^5 - 2x_2^5x_3^4 \tag{1.5}$$

$$2x_1^2x_2x_3^2 + x_2^4x_3^5 - x_2^6x_3^2 + 4x_1x_2^2x_3^5 - 2x_2^5x_3^4 - (f \cdot 4x_3^5) =$$
$$= 2x_1^2x_2x_3^2 + x_2^4x_3^5 - x_2^6x_3^2 - 2x_2^5x_3^4 + 8x_1x_2x_3^7 - 4x_2^4x_3^6$$

Старшая степень системы f одночлен $x_1x_2^2$, каждый одночлен из полученного многочлена не делится на эту старшую степень, получаем, полученный многочлен есть искомый остаток. Запишем многочлен в лексикографическом порядке.

$$2x_1^2x_2x_3^2 + 8x_1x_2x_3^7 + x_2^4x_3^5 - x_2^6x_3^2 - 2x_2^5x_3^4 - 4x_2^4x_3^6 \tag{1.6}$$

Ответ:

$$2x_1^2x_2x_3^2 + 8x_1x_2x_3^7 + x_2^4x_3^5 - x_2^6x_3^2 - 2x_2^5x_3^4 - 4x_2^4x_3^6 \tag{1.7}$$

Проделанный алгоритм схож с алгоритмом Евклида [5].

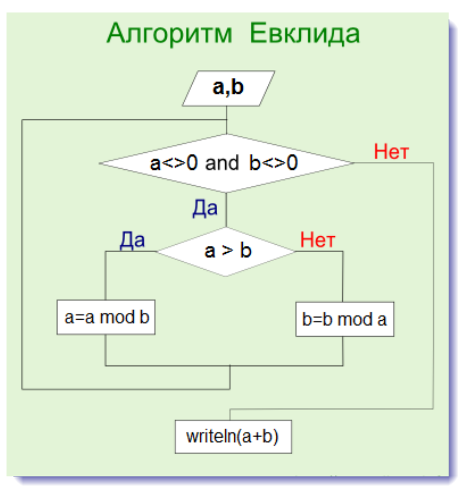

Рис. 1.4: Алгоритм Евклида

1.4 Задание 3

Выясните, является ли множество $\{f_1, f_2, f_3\}$ системой Грёбнера, где

$f_1 = 2x_1x_2+4x_1x_3+x_2x_3^2$ $\qquad f_2 = 4x_1x_3^2+x_2x_3^3-4$ $\qquad f_3 = x_2^2x_3^3-4x_2-8x_3$

Система F является системой Гребнера, если полином [2] S всех попарных f редуцируется к 0 относительно F. Всего таких паросочетаний 9 штук, из них пары $S(f_i, f_i)$ точно редуцируются к 0, а полиномы вида $S(f_i, f_j)$ $= -S(f_j, f_i)$, i $>$ j. Докажем, что полиномы $S(f_i, f_j)$ редуцируются к 0 относительно F. Это полиномы $S(f_1, f_2), S(f_1, f_3), S(f_2, f_3)$, каждый полином находится через умножение первого многочлена на старшую степень и вычитание второго многочлена, умноженного на старшую степень. С помощью элементарных редукций относительно F, полученные многочлены можно привести к 0, т.е. они редуцируются к 0 относительно F. Осталось показать, что оставшиеся полиномы $-S(f_j, f_i)$ тоже редуцируются к 0, в силу того, что они равны $S(f_i, f_j) = -S(f_j, f_i)$. Получаем, что полиномы всех пар f редуцируются к 0, значит F - система Гребнера.

1.5 Задание 4

Докажите, что множество $F \subseteq K[x] \setminus \{0\}$ является системой Грёбнера тогда и только тогда, когда существует такой многочлен $f \in F$, который делит любой многочлен из F.

1. (a) Пусть данный многочлен f есть f_i, чтобы доказать, что F система Гребнера, воспользуемся предыдущим утверждением, что все f из F, редуцируются к 0 относительно F и для цепочек элементарных редукций остаток многочлена относительно F определен однозначно. Рассмотри полиномы $S(f_i, f_j)$, $f_i, f_j \in F$, пусть степень i минимально, тогда НОК старших степеней будет равен j, потому что рассматриваемые многочлены от одной переменной. Полином S будет иметь следующий вид.

   (b)
   $$S(f_i, f_j) = x^{j-i} f_i - f_j \tag{1.8}$$

   (c) Теперь докажем, что такие полиномы редуцируются к 0 относительно F. Каждую элементарную редукцию будем проводить по многочлену f.

   (d)
   $$x^{j-i} f_i - f_j + (d_1 f) + (d_2 f) + ...(d_k f) = 0 \tag{1.9}$$

   (e) Получаем, что такими редукциями любой полином редуцируется к 0 относительно F. Также можно однозначно определить остаток таких цепочек относительно F, который равен 0 и не зависит от выбора преобразования. Если взять остаток относительно f в равенстве сверху, то получим, что f_j делимо f, также делимы будут полиномы $S(f_i, f_j)$ относительно f.

2. Получаем, что система F есть система Гребнера [4].

Литература

[1] Эрнест Винберг. *Курс алгебры.* Litres, 2022.

[2] Валерий Николаевич Докин, ВД Жуков, НА Колокольникова, ОВ Кузьмин, and МЛ Платонов. Комбинаторные числа и полиномы в моделях дискретных распределений. 1990.

[3] Владимир Александрович Ильин and Галина Динховна Ким. Линейная алгебра и аналитическая геометрия. *М.: Изд-во Моск. ун-та*, 1998.

[4] Анатолий Николаевич Корюкин. Базисы Грёбнера–Ширшова алгебры Ли. *Алгебра и логика*, 44(2):131–147, 2005.

[5] Владимир Николаевич Крупский and Валерий Егорович Плиско. Теория алгоритмов. *М.: Academia*, 2009.