6 Поля Галуа

I. Множество $GF(p) = \{0, 1, \ldots, p-1\}$ с операциями сложения $+$ и умножения $\cdot$ по модулю простого числа p является *простым полем. Кольцо многочленов* $F[x]$ состоит из всех многочленов от переменной x с коэффициентами из поля $GF(p)$. Рассмотрим множество K всех корней многочлена $x^{p^m} - x$ над полем $GF(p)$.

6.1 Доказать, что K является полем.

6.2 Доказать, что все корни многочлена $x^{p^m} - x$ различны, и следовательно $|K| = p^m$.

Построенное поле K называется *расширением Галуа* поля $GF(p)$ и обозначается $GF(p^m)$. Оно содержит $GF(p)$ в качестве наименьшего подполя, число p называется его *характеристикой*. Поле $GF(p^m)$ можно рассматривать как m-мерное векторное пространство над $GF(p)$. В случае $p = 2$ оно совпадает с двоичным кубом E^m. Отличие заключается в том, что теперь, кроме операций сложения векторов из $GF(p^m)$ и умножения их на скаляр из $GF(p)$, будет определена новая операция — умножение векторов.

6.3 Доказать, что в поле характеристики p справедливо равенство $(x-y)^p = x^p - y^p$.

II. *Порядком* элемента β конечного поля называется наименьшее целое положительное число k такое, что $\beta^k = 1$.

6.4 Пусть элементы β и γ коммутативной группы имеют порядки m и n соответственно, причем $(m, n) = 1$. Доказать, что порядок элемента $\beta \cdot \gamma$ равен mn.

6.5 Пусть порядок элемента β коммутативной группы равен n. Доказать, что порядок элемента β^k равен $\frac{n}{(n,k)}$.

Ненулевые элементы поля $GF(p^m)$ образуют циклическую группу $\{1, \alpha, \alpha^2, \ldots, \alpha^{p^m-2}\}$. Порождающий элемент этой группы (например α) называется *примитивным элементом* поля. Многочлен $g(x) \in F[x]$, корнем которого является примитивный элемент поля, называется *примитивным*.

Теорема Ферма. *Каждый элемент β поля $GF(p^m)$ является корнем уравнения $x^{p^m} - x = 0$.*

III. Многочлен $g(x) \in F[x]$ *неприводим* над $GF(p)$, если он не может быть представлен в виде произведения двух многочленов из $F[x]$ меньшей степени. С помощью неприводимого над $GF(p)$ многочлена $g(x)$ степени m можно построить поле Галуа следующим образом: $GF(p^m)$ есть факторкольцо кольца $F[x]$ по модулю $g(x)$.

Функция Мёбиуса $\mu(m) = \begin{cases} 1, & \text{если } m = 1; \\ (-1)^r, & \text{если } m \text{ — произведение } r \text{ различных простых чисел;} \\ 0, & \text{в остальных случаях.} \end{cases}$

Для числа нормированных неприводимых многочленов над $GF(p)$ степени m справедлива формула $I_m = \frac{1}{m} \sum\limits_{d,\, d|m} \mu(d) p^{m/d}$.

Многочлен $x^{p^m} - x$ равен произведению всех нормированных неприводимых над $GF(p)$ многочленов, степени которых делят m.

6.6 Найти все неприводимые над $GF(2)$ многочлены степени, не превышающей 3.

6.7 Построить поле Галуа $GF(2^2)$, используя неприводимый многочлен $x^2 + x + 1$. Найти таблицы сложения и умножения элементов поля.

6.8 Построить два представления поля Галуа $GF(2^3)$, используя один неприводимый многочлен $x^3 + x + 1$ и разные примитивные элементы. Указать изоморфизм этих представлений.

6.9 Найти число I_4 неприводимых многочленов над $GF(2)$ степени 4.

6.10 Доказать, что многочлен $M(x) = x^5 + x^2 + 1$ неприводим над $GF(2)$.

6.11 Найти разложения многочленов на неприводимые над $GF(2)$ множители:
а) $f(x) = x^5 + x^4 + x^2 + x$;
б) $g(x) = x^{16} - x$.

6.12 Построить поля Галуа
а) $GF(2^3)$, используя неприводимый многочлен $x^3 + x^2 + 1$. Показать изоморфизм между построенным полем и полем из задачи 6.8.
б) $GF(3^2)$, используя неприводимый многочлен $x^2 + x + 2$.
в) $GF(3^3)$, используя неприводимый многочлен $x^3 + 2x + 1$.

Теория к Семинару 7 "Циклические коды".
I. Определение циклического кода. Теорема о циклическом коде и идеале кольца $F[x]/(x^n - 1)$. Порождающий многочлен циклического кода. Представление произвольного кодового многочлена циклического кода в виде произведения некоторого многочлена на порождающий. Порождающая матрица циклического кода. Проверочный многочлен и проверочная матрица циклического кода. В каком случае могочлен $g(x)$ может быть порождающим многочленом некоторого циклического кода? Число циклических кодов фиксированной длины.
II. Кодирование циклических кодов. Систематический код. Первый и второй систематические кодеры. Несистематический кодер.
III. Минимальный многочлен элемента поля. Свойства минимального многочлена.