ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 21 МАТЕМАТИКИ Выпуск 5
2014

А. В. Анашкин (Москва, ТВП). **Об изоморфизме графов двух преобразований.**

Пусть $\tau : GF(q)[x] \to GF(q)[x]$ отображение кольца многочленов над полем из q элементов в себя, задаваемое формулой $\tau(\sum_{i=0}^{d} a_i x^i) = \sum_{i=0}^{d} a_i x^{q^i}$.

Известны следующие свойства отображения τ ([1]).

1) τ — инъективное отображение и, в частности, $\tau : P[x] \to \tau(P[x])$ — изоморфизм векторных пространств.

2) Для любых многочленов $h(x), g(x) \in P[x]$ равносильны условия $g(x)|h(x)$ и $\tau(g(x))|\tau(h(x))$.

3) Если многочлен $f(x) = \sum_{i=0}^{n} f_i X^i$ удовлетворяет условию $f(0) \neq 0$, то многочлен $\tau(f(x))$ не имеет кратных корней в поле разложения. Если многочлен $f(x)$ имеет вид $f(x) = h(x) \cdot x^t$, где $h(0) \neq 0$ и $t \geqslant 1$, то $\tau(f(x)) = (\tau(h(x))^{q^t}$.

Пусть далее многочлен $f(x)$ имеет вид $f(x) = x^n - \sum_{i=0}^{n-1} f_i x^i$ и пусть V_n — множество n-мерных векторов над полем $GF(g)$. Зададим $T : V_n \to V_n$ линейное преобразование пространства V_n, положив $T(a_{n-1}, a_{n-2}, \ldots, a_1, a_0) = (\sum_{i=0}^{n-1} f_i a_i, a_{n-1}, a_{n-2}, \ldots, a_1)$.

Обозначим через P^* поле разложения многочлена $F(x) = \tau(f(x))$. Определим отображение $\sigma : P^* \to P^*$, положив $\sigma(a) = a^q$, $a \in P^*$. Отображение σ является автоморфизмом векторного пространства $P^*_{GF(q)}$. Пусть $M = \{\alpha \in P^* | F(\alpha) = 0\}$ — множество корней многочлена $F(x) = \tau(f(x))$ в поле разложения P^*. Отображение σ является также и автоморфизмом векторного пространства $M_{GF(q)}$.

Пусть целое неотрицательно число t является максимальным со свойством $x^t | f(x)$, и пусть также MR — это множество корней многочлена $F(x)$ с учетом их кратности. Множество MR можно рассматривать в виде декартового произведения двух множеств $MR = \{(\alpha, s) | \alpha \in M, s \in \{1, 2, \ldots, q^t\}\} = M \times \{1, 2, \ldots, q^t\}$.

Через S_{q^t} будем обозначать множество всех подстановок на множестве чисел $\{1, 2, \ldots, q^t\}$.

Утверждение. *В условиях введенных выше обозначений для произвольной подстановки $\pi \in S_{q^t}$ существует биективное отображение $A : V_n \to MR$ такое, что для любого вектора $a \in V_n$ справедливо $A(T(a)) = (\sigma, \pi)(A(a))$.*

Следствие 1. *Для произвольной подстановки $\pi \in S_{q^t}$ граф преобразования T на множестве V_n изоморфен графу преобразования (σ, π) на множестве MR.*

Следствие 2. *В случае, если $t = 0$, то изоморфны графы двух линейных преобразований — преобразования T на множестве V_n и преобразования σ на множестве M.*

СПИСОК ЛИТЕРАТУРЫ

1. Лидл Р., Нидеррайтер Г. Конечные поля. М.: 1988.