СУЩЕСТВЕННО РАЗЛИЧНЫЕ НЕПРИВОДИМЫЕ МНОГОЧЛЕНЫ НАД КОНЕЧНЫМИ ПОЛЯМИ

Стефан М. Додунеков

§ 1. Предварительные сведения

В работе используются следующие обозначения:

$GF(q)$ — поле Галуа порядка q, q — простое число,

$GF(q)[z]$ — кольцо многочленов от одной переменной с коэффициентами из $GF(q)$,

Q_m — подмножество $GF(q)[z]$, составленное из всех неприводимых над $GF(q)$ многочленов степени m,

P_m — множество нормированных многочленов из Q_m,

U — группа линейных трансформаций вида $u: z \to az + b$, $a, b \in GF(q)$, $a \neq 0$,

$u_1, \ldots, u_2 \; u_{q(q-1)}$ — элементы U,

T — подгруппа группы U, составленная из линейных трансформаций вида $\tau: z \to z + b$, $b \in GF(q)$,

$\tau_1, \tau_2, \ldots, \tau_q$ — элементы T,

V — подгруппа группы U, составленная из линейных трансформаций вида $v: z \to az$, $a \in GF(q)$, $a \neq 0$,

$v_1, v_2, \ldots, v_{q-1}$ — элементы V,

$f(u(z))$ — многочлен, полученный из $f(z) \in GF(q)[z]$ через $u: z \to az + b$.

Пусть группа G действует на множестве S ([1], 32). S распадается на непересекающиеся классы G — эквивалентных между собой элементов, называемых орбитами множества S относительно группы G.

Определение. Два элемента из S называются существенно различными относительно G, если принадлежат разным орбитам множества S относительно группы G.

§ 2. Нормированные линейные трансформации

Если $f(z) \in P_m$, то и $f(\tau(z)) \in P_m$. Из равенств $f(\tau_i(\tau_j(z))) = f(\tau_i \tau_j(z))$ и $f(1.z) = f(z)$, верных для любых $\tau_i, \tau_j \in T$ и $f(z) \in P_m$, следует, что T действует на множестве P_m.

Лемма 1. В каждой орбите P_m относительно T содержатся или один, или q многочленов.

Доказательство. Число элементов в каждой орбите есть индекс некоторой подгруппы группы T и делит ее порядок. Но T — группа простого порядка q. Следовательно, или все многочлены $f(\tau_1(z))$, $f(\tau_2(z)), \ldots, f(\tau_q(z))$ различны между собой, или совпадают.

Следствие. Многочлен $f(z) \in P_m$ порождает тривиальную орбиту (орбиту из одного элемента) относительно T тогда и только тогда, когда $f(z+1)=f(z)$.

Пусть I_m число многочленов, а J_m — число орбит относительно T в P_m.

Теорема 1. Если $q>2$, то q не делит I_m тогда и только тогда, когда m имеет каноническое разложение $m=q\,p_1\,p_2\ldots p_s$. Если $q=2$, то I_m нечетное тогда и только тогда, когда m имеет каноническое разложение $m=2^\lambda\,p_1\,p_2\ldots p_s$, $\lambda=1, 2$.

Доказательство. Известна следующая формула ([2], 93):

$$I_m=\frac{1}{m}\sum_{d\mid m}\mu(d)\,q^{\frac{m}{d}}. \tag{1}$$

Здесь $\mu(d)$ — функция Мебиуса. Пусть $m=q^\lambda\,p_1^{l_1}\,p_2^{l_2}\ldots p_s^{l_s}$ — каноническое разложение числа m на простые сомножители. Тогда $\mu(d)=0$ для каждого делителя $d=q^\nu\,p_1^{l_1}\,p_2^{l_2}\ldots p_s^{l_s}$ числа m, в котором хотя бы один из показателей $\nu, l_1, l_2, \ldots, l_s$ по меньшей мере равен двум. Наибольший делитель, для которого $\mu(d)\neq 0$, есть $d_{\max}=q\,p_1\,p_2\ldots p_s$ и наименьшая степень числа q, которая участвует в сумме (1), есть $q^{q^{\lambda-1}p_1^{l_1-1}p_2^{l_2-1}\ldots p_s^{l_s-1}}$. Следовательно

$$I_m=\frac{1}{m}\left(q^{q^{\lambda-1}p_1^{l_1-1}p_2^{l_2-1}\ldots p_s^{l_s-1}}+\sum_{\substack{d\mid m\\ d\neq d_{\max}}}\mu(d)\,q^{q^{\lambda-\nu}p_1^{l_1-l_1}p_2^{l_2-l_2}\ldots p_s^{l_s-l_s}}\right)$$

$$=\frac{q^{q^{\lambda-1}p_1^{l_1-1}p_2^{l_2-1}\ldots p_s^{l_s-1}}}{q^{\lambda}p_1^{l_1}p_2^{l_2}\ldots p_s^{l_s}}\cdot(1+Kq).$$

Так как I_m целое число, всегда

$$\lambda\leqq q^{\lambda-1}p_1^{l_1-1}p_2^{l_2-1}\ldots p_s^{l_s-1}. \tag{2}$$

Если $q>2$, равенство в (2) возможно только при $\lambda=1$, $l_1=l_2=\ldots=l_s=1$. Если $q=2$, оно выполняется только при $\lambda=1$, $l_1=l_2=\ldots l_s=1$ и $\lambda=2$, $l_1=l_2=\ldots=l_s=1$.

Теорема доказана.

Следствие. Если $m=q\,p_1\,p_2\ldots p_s$ и $I_m=nq+l$, $0<l<q$, то существуют по меньшей мере l тривиальных орбит множества p_m от-

носительно T. Если $q=2$, такая орбита существует и при $m=4p_1p_2\ldots p_s$.

Пусть многочлен $f(z)=z^m+a_1z^{m-1}+\ldots+a_m$ из P_m порождает тривиальную орбиту. По следствию к лемме 1 $f(z)=f(z+1)$. Отсюда следует, что $f(z)$ порождает тривиальную орбиту тогда и только тогда, когда выполняются равенства

$$
\begin{aligned}
&\binom{m}{1}+a_1=a_1,\\
&\binom{m}{2}+a_1\binom{m-1}{1}+a_2=a_2,\\
&\ldots\ldots\ldots\ldots\\
&\binom{m}{k}+a_1\binom{m-1}{k-1}+a_2\binom{m-2}{k-2}+\ldots+a_{k-1}\binom{m-k+1}{1}+a_k=a_k,\\
(3)\qquad &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\binom{m}{m-1}+a_1\binom{m-1}{m-2}+a_2\binom{m-2}{m-3}+\ldots+a_{m-1}=a_{m-1},\\
&1+a_1+a_2+\ldots+a_{m-1}+a_m=a_m.
\end{aligned}
$$

Теорема 2. Если $(m, q)=1$, все орбиты множества P_m относительно группы T являются нетривиальными и $J_m=\frac{1}{q}I_m$.

Доказательство. Первое равенство в (3) показывает, что необходимым условием для существования орбиты из одного многочлена есть $(m, q)=q$.

Теорема 3. Если $m=q$, то $J_m=q^{q-2}+q-2$.

Доказательство. При $q=m$ из (3) однозначно определяются коэффициенты $a_1, a_2, \ldots, a_{m-1}$. И так как $0\leqslant a_m<q$, то существуют не больше чем $q-1$ орбит из одного многочлена. Пусть n число нетривиальных, а l — число тривиальных орбит. Тогда $I_m=nq+l$ с $0<l<q$. Но при $m=q$ $I_m=q^{q-1}-1=(q^{q-2}-1)q+q-1$. Следовательно $n=q^{q-2}-1$, $l=q-1$, $J_m=n+l=q^{q-2}+q-2$.

Мы показали, что при $(m, q)=1$ существуют $J_m=\frac{1}{q}I_m$ существенно различных относительно T многочленов (при $m=q$ их число $J_m=q^{q-2}+q-2$), а все остальные можно получить из этих существенно различных с помощью трансформации с элементами группы T.

§ 3. Линейные трансформации

Если $f(z)\in Q_m$, то $f(u(z))\in Q_m$. Из равенств $f(u_i(u_j(z)))=f(u_iu_j(z))$ и $f(1+z)=f(z)$, верных для любых $u_i, u_j\in U$ и $f(z)\in Q_m$, следует, что U действует на Q_m. Предположим теперь, что $q>2$ (при $q=2$ U совпадает с T). Каждую трансформацию $u: z\to az+b$ можно единственным образом представить как произведение двух трансформаций $\tau: z\to z+b$

и $v: z \to az$, $\tau \in T$, $v \in V$ и $v_i \tau_j$ для $i=1, 2, \ldots, q-1$, $j=1, 2, \ldots, q$ — все элементы группы U.

Лемма 2. Пусть $f(z)=a_0 z^m + a_1 z^{m-1} + \ldots + a_m \in Q_m$. Все многочлены $f(v_1(z)), f(v_2(z)), \ldots, f(v_{q-1}(z))$ различны.

Доказательство. Если в равенстве $f(az)=f(bz)$ сравним коэффициенты перед z, получим, что $a=b$.

Так как при доказательстве леммы 1 мы не использовали нормированности многочленов, можно сформулировать:

Лемма 3. Любая орбита множества Q_m относительно T содержит или один, или q элементов.

Следствие. Многочлен $f(z) \in Q_m$ порождает тривиальную орбиту множества Q_m относительно T тогда и только тогда, когда $f(z) = f(z+1)$.

Теорема 4. Каждая орбита множества Q_m относительно U содержит или $q-1$, или $q(q-1)$ многочленов. Если $f(z) \in Q_m$ порождает тривиальную орбиту относительно T, он содержится в орбите из $q-1$ элементов относительно U. Если $f(z)$ порождает нетривиальную орбиту относительно T, содержится в орбите из $q(q-1)$ элементов относительно U.

Доказательство. Порядок U равен $q(q-1)$. Порядок каждой орбиты как индекс некоторой подгруппы группы U делит $q(q-1)$. Пусть $f(z) \in Q_m$ порождает орбиту

$$f(u_1(z)),\ f(u_2(z)), \ldots,\ f(u_{q(q-1)}(z)) \tag{4}$$

относительно U. Если $f(z)$ содержится в тривиальной орбите Q_m относительно T, в (4) согласно лемме 2 только $q-1$ из многочленов различны. Если $f(z)$ из нетривиальной орбиты множества Q_m относительно T, в (4) V действует на q различных многочленов

$$g_1(z),\ g_2(z), \ldots,\ g_q(z). \tag{5}$$

В этом случае в (4) или $q-1$, или $q(q-1)$ различных многочленов. Но если они только $q-1$, выходит, что многочлены (5) (число их q) лежат в одной орбите Q_m относительно V, а V — группа порядка $q-1$. Следовательно все многочлены в (4) различны.

Следствие. Если $(m, q)=1$, все орбиты в Q_m относительно U содержат по $q(q-1)$ элементов и число орбит равно J_m.

Иными словами, можно выбрать J_m существенно различных многочленов и трансформируя их с элементами U, получить все многочлены Q_m.

Пусть в P_m существуют тривиальные орбиты относительно T. В таком случае необходимо $(m, q)=q$.

Теорема 5. Если $\varphi_1(z), \varphi_2(z), \ldots, \varphi_l(z)$ — все многочлены, принадлежащие тривиальным орбитам множества P_m относительно T и $(m, q-1)=1$, то

$$
(6)\qquad
\begin{array}{l}
\varphi_1(v_1(z)),\quad \varphi_1(v_2(z)),\ldots,\ \varphi_1(v_{q-1}(z)),\\
\varphi_2(v_1(z)),\quad \varphi_2(v_2(z)),\ldots,\ \varphi_2(v_{q-1}(z)),\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\varphi_l(v_1(z)),\quad \varphi_l(v_2(z)),\ldots,\ \varphi_l(v_{q-1}(z))
\end{array}
$$

— все орбиты множества Q_m относительно U, составленные из $q-1$ элементов.

Доказательство. Все орбиты в (6) различны. Действительно, если две из них совпадают, скажем i-тая и j-тая, следовало бы, что для некоторого $a \in \mathrm{GF}(q)$ $\varphi_j(z)=\varphi_i(az)$. Сравнивая старшие коэффициенты многочленов $\varphi_j(z)$ и $\varphi_i(az)$, получим, что $a^m=1$. Но так как и $a^{q-1}=1$, а $(m, q-1)=1$, выходит, что $a=1$. Следовательно, все многочлены в (6) различны. Но каждый из них можно записать в виде $a\varphi_i(z)$ с $a \in \mathrm{GF}(q)$. Число различных многочленов такого вида есть $l(q-1)$. Таким образом, мы показали, что (6) совпадает с множеством всех многочленов вида $a\varphi(z)$, $a \in \mathrm{GF}(q)$, $a \neq 0$, $\varphi(z)$ — многочлен из тривиальной орбиты множества P_m относительно T. С другой стороны, если $g(z) \in Q_m$ лежит в орбите из $q-1$ элементов относительно U, в представлении $g(z)=a\varphi(z)$ с $a \in \mathrm{GF}(q)$, $a \neq 0$, $\varphi(z) \in P_m$ согласно теореме 4 $\varphi(z)$ лежит в тривиальной орбите относительно T. Это показывает, что $g(z)$ лежит в некоторой орбите из (6).

Следствие. Если $m=q$, существуют точно $q-1$ орбит из $q-1$ элементов и $q^{q-2}-1$ орбит из $q(q-1)$ элементов.

§ 4. Примеры

Пусть $q=3$. $l_1=3$, $J_1=1$. $l_2=3$, $J_1=1$. Нормированные неприводимые многочлены x^2+1, x^2+x+2, x^2+2x+2 лежат в одной орбите относительно T.

$l_3=8$, $J_3=4$. В этом случае две из орбит тривиальны:

$$A_1=\{x^3+2x+1\},\quad A_2=\{x^3+2x+2\},$$

$$A_3=\{x^3+x^2+2,\ \ x^3+x^2+x+2,\ \ x^3+x^2+2x+1\},$$

$$A_4=\{x^3+2x^2+1,\ \ x^3+2x^2+x+1,\ \ x^3+2x^2+2x+2\}.$$

$l_4=18$, $J_4=6$. Здесь $(m, q)=(4, 3)=1$ и поэтому все орбиты нетривиальны:

$$A_1=\{x^4+x+2,\ \ x^4+x^3+2x+1,\ \ x^4+2x^3+2\},$$

$$A_2=\{x^4+x^2+2,\ \ x^4+x^3+x^2+1,\ \ x^4+2x^3+x^2+1\},$$

$$A_3=\{x^4+x^2+x+1,\ \ x^4+x^3+x^2+x+1,\ \ x^4+2x^3+x^2+x+2\},$$

$$A_4=\{x^4+x^3+2,\ \ x^4+2x^3+x+1,\ \ x^4+2x+2\},$$

$$A_5=\{x^4+2x^2+2,\ \ x^4+x^3+2x^2+2x+2,\ \ x^4+2x^3+2x^2+x+2\},$$

$$A_6=\{x^4+x^2+2x+1,\ \ x^4+x^3+x^2+2x+2,\ \ x^4+2x^3+x^2+2x+1\}.$$

§ 5. Замечание

Используя результаты для группы U, легко можно рассмотреть действие группы невырожденных дробно линейных трансформаций на множестве Q_m.

ЛИТЕРАТУРА

1. Ленг, С.: Алгебра. „Мир", М., 1968.
2. Берлекэмп, Э.: Алгебраическая теория кодирования. „Мир", М., 1971.

Поступила на 11. IX. 1972 г.

ESSENTIALLY DIFFERENT IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS

S. M. Dodunekov

(SUMMARY)

Notations:

Q_m — the set of all irreducible polynomials over GF(q) (q — prime number) of degree m,

P_m the set of normed polynomials in Q_m,

U the group of linear transformations $u: z \to az+b$, $a, b \in$ GF(q), $a \neq 0$,

V the subgroup of U, containing elements with $b=0$,

T — the subgroup of U with elements $\tau: z \to z+b$, $v_1, v_2, \ldots, v_{q-1}$ — the elements of V,

$I_m = \dim P_m$,

J_m — the number of orbits in P_m relative to T.

The following results are proved:

1. If $m=q\,p_1\,p_2\ldots p_s$ and $I_m=nq+l$, $0<l<q$, then there exist at least l trivial orbits of P_m relative to T. If $q=2$, such orbit exists if $m=2^\lambda\,p_1\,p_2\ldots p_s$, $\lambda=1, 2$.

2. Theorem 2. If $(m, q)=1$, then all orbits of P_m relative to T are nontrivial and $J_m=\frac{1}{q}\,I_m$.

3. Theorem 3. If $m=q$, then $J_m=q^{q-2}+q-2$.

4. If $(m, q)=1$, then every orbit of Q_m relative to U contains $q(q-1)$ elements and the number of orbits is J_m.

5. Theorem 5. If $\varphi_1(z), \varphi_2(z), \ldots, \varphi_l(z)$ are all trivial orbits of P_m relative to T and $(m, q-1)=1$, then

$$\begin{array}{llll}
\varphi_1(v_1(z)), & \varphi_1(v_2(z)) & , \ldots, & \varphi_1(v_{q-1}(z)), \\
\varphi_2(v_1(z)), & \varphi_2(v_2(z)) & , \ldots, & \varphi_2(v_{q-1}(z)), \\
\cdot & \cdot & \cdot & \cdot \\
\varphi_l(v_1(z)), & \varphi_l(v_2(z)) & , \ldots, & \varphi_l(v_{q-1}(z))
\end{array}$$

are all orbits of Q_m relative to U, which contain $q-1$ elements.

6. If $m=q$, then there exist exactly $q-1$ orbits with $q-1$ elements.