ЗА ЕДЕН ВИД ПОЛИЊА СО КОНЕЧНА КАРАКТЕРИСТИКА

Ѓорги Чупона

1. (i) Ако постои прост број p таков да е $pa=0$, за секој елемент a од некое поле K, се вели дека полето K има конечна карактеристика p. Секое конечно поле има конечна карактеристика; бројот на елементите од некое конечно поле со карактеристика p е од облик p^α, каде α е природен број ([1], стр. 116).

(ii) Изоморфните полиња, како што е вообичаено, не ги сметаме за различни. Затоа: за секој пар броеви p и α, каде p е прост, а α природен, постои само едно поле со p^α елементи — полето што се добива кога полето од класи на остатоци мод p се прошири со корените на равенката $x^{p^\alpha}-x=0$ ([1], стр. 116).

(iii) Секоја конечна подмножина од некое поле K, која е затворена во однос на собирање и множење е потполе од K.

Пресекот од сите потполиња на полето K се вика просто потполе. Полето од класи на остатоци mod p е просто потполе за секое поле со карактеристика p ([1], стр. 92).

(iv) Групата чиј секој елемент има за ред некоја степен од простиот број q се вика q-група. Секоја конечна q-група има q^β елементи, а важи и обратното ([2], стр. 175).

2. Со K_{pq} ќе го означуваме секое поле што има карактеристика p, а мултипликативна q-група. Целта на овој прилог е да го докажеме следниот став:

Облик K_{pq} *имаат само:* a) *полето од класи на остатоци* mod p, *ако е* $p=2^{2^k}+1$ Fermat-ов *прост број;* b) *полето со* 2^α *елементи, ако е* $q=2^\alpha-1$ Mersenne-ов *прост број;* c) *полето со 9 елементи.*

Дека се тие полиња од облик K_{pq} и тоа по ред: K_{p2}, K_{2q}, K_{32}, е очигледно. Ќе покажеме дека не постојат други полиња од тој вид. Напоменуваме дека полето од класи на остатоци mod 2, т. е. полето $\{0, 1\}$, не го сметаме за поле K_{2q}.

Лема 1. *Секое поле* K_{pq} *има конечно потполе* K'_{pq}.

За $p\neq 2$ такво е барем простото потполе, а за $p=2$ множината што ги содржи сите елементи од облик

$$(1) \qquad u_j = \sum_{i=1}^{q^\nu} \varepsilon_{ij}\, a^i,$$

каде е: $\varepsilon_{ij} = 0$ или 1, $a \neq 0,1$, q^ν мултипликативен ред на a. Дека таа множина е потполе следува од (iii), бидејќи е очигледно конечна и затворена во однос на собирање и множење; таа не се совпаѓа со потполето $\{0, 1\}$, оти ги содржи сите степени a^i од a.

Лема 2: *За дадено поле K_{pq} постои барем еден пар природни броеви α и β кои, заедно со p и q, ја задоволуваат релацијата*

$$(2) \qquad p^\alpha = q^\beta + 1.$$

Навистина, ако K'_{pq} е конечно потполе од полето K_{pq}, тоа има p^α, а неговата мултипликативна група, спрема (iv), q^β елементи.

Лема 3. *Релацијата (2) е исполнета само ако е:*

a) $p = 2^{2^k} + 1$, $q = 2$, $\alpha = 1$, $\beta = 2^k$; b) $p = 2$, $q = 2^\alpha - 1$, $\beta = 1$; c) $p = 3$, $q = 2$, $\alpha = 2$, $\beta = 1$.

Точноста на оваа лема следува од еден став на J. W. S. Cassels ([3], стр. 161, Theorem IV), а лесно се докажува и директно.

Од лемите 2 и 3 непосредно следува:

Лема 4. *Поле K_{pq} постои само ако е $p = 2^{2^k} + 1$, а $q = 2$ или $p = 2$, а $q = 2^\alpha - 1$.*

Лема 5. *Секое конечно потполе од полето K_{2q} (K_{p2}, $p \neq 3$) има $q+1$ (p) елементи; полето K_{32} може да содржи конечни потполиња со 9 или 3 елементи.*

Споменатото досега за конечни потполиња од било кое поле K_{pq} важи, несомнено, и за секое конечно поле K_{pq}. Затоа од последната лема, бидејќи спрема (ii) со бројот на елементите полето е наполно одредено, следува точноста на ставот за конечните полиња K_{pq}.

Лема 6. *Секое поле K_{pq} е конечно.*

Доказ. Нека е K'_{pq} некое максимално конечно потполе од полето K_{pq}, т. е. K'_{pq} не е право потполе од друго конечно потполе на K_{pq}; дека такво постои се гледа од лемите 1 и 5. Да ја разгледаме множината M на сите елементи од облик

$$(3) \qquad v_j = \sum_{i=1}^{q^\mu} \eta_{ij}\, b^i,$$

каде η_{ij} е произволен елемент од K'_{pq}, а b од K_{pq} со мултипликативен ред q^{μ}. Таа е потполе од K_{pq}, оти е, очигледно, конечна и затворена во однос на собирање и множење; освен тоа, очигледно е и дека b, а и сите елементи од K'_{pq}, ѝ припаѓаат на M. Значи K'_{pq} е потполе од конечното потполе M, а тоа е можно само ако е $K'_{pq} = M$, од каде, бидејќи произволен елемент b од K_{pq} припаѓа на K'_{pq}, следува $K_{pq} = K'_{pq}$. Со тоа лемата, а и целиот став се докажани.

Да напоменеме на крајот дека во литературата, достапна за нас, не сме сретнале полиња од облик K_{pq}.

ЛИТЕРАТУРА

[1] *B. L. van der Waerden*, Modern Algebra, vol. I, New York 1953.

[2] *A. G. Kurosch*, Gruppentheorie, Berlin 1953.

[3] *J. W. S. Cassels*, On the equation $a^x - b^y = 1$, American Journal of Mathematics, vol. 75 (1953) p. 159—162.

Summary

ON FIELDS WITH FINITE CHARACTERISTIC

G. Čupona

In this note we prove that unique fields with characteristic p and multiplplicative q-group are:

a) The residue class ring modulo p, if $p=2^{2^k}+1$ is a prime,

b) The field with 2^{α} elements, if $q=2^{\alpha}-1$ is a prime and

c) The field with 9 elements.