

ЗА ПЕРИОДИЧНИТЕ ПОЛИЊА

Г. ЧУПОНА

За полето P велеме дека е периодично ако е периодична неговата мултипликативна група, т. е. ако за секој елемент $x (\neq 0)$ од P постои природен број n таков да $x^n = 1$. Со $n(x)$ ќе го означуваме најмалиот природен број со таа особина, а со $v(n)$ бројот од сите различни прости делители на n .

Јасно е дека функцијата $v(n(x))$ е ограничена во случај кога полето P е конечно. Целта на оваа работа е да докажеме дека важи и обратното, т. е. точноста на следната

Теорема. *Ако функцијата $v(n(x))$ е ограничена во периодичното поле P , тогаш P е конечно.*

При доказот на теоремата ќе ги користиме наредните две лема.

Лема 1. Ако $a > 1$, m и n се природни броеви, тогаш

$$(1) \quad a^m - 1 \equiv 0 \pmod{a^n - 1} \Leftrightarrow m \equiv 0 \pmod{n}.$$

Лема 2. Ако a и r се природни броеви поголеми од 1, тогаш

$$(2) \quad v(a-1) = v(a^r - 1) \rightarrow r = 2, \quad a \equiv 1 \pmod{2}, \quad a \not\equiv 1 \pmod{4}.$$

Точноста на тие лема се докажува лесно. Имено, првата се добива од равенството

$$a^m - 1 = (a-1) [(1+a+\dots+a^{n-1})(1+a^n+a^{2n}+\dots+a^{(k-1)n}) + a^{kn}(1+a+a^2+\dots+a^{r-1})]$$

каде $m = kn + r$ и $0 < r \leq n$.

Ќе споменеме сега еден начин за докажувањето на втората лема. Нека претпоставиме дека

$$(3) \quad a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} + 1$$

и

$$(4) \quad a^2 = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k} + 1$$

каде $\alpha_i, \beta_j > 0$, а p_1, p_2, \dots, p_k се различни прости броеви. Од (3) и (4), после степенување и кратење, се добива

$$(5) \quad p_1^{\beta_1 - \alpha_1} p_2^{\beta_2 - \alpha_2} \dots p_k^{\beta_k - \alpha_k} = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} + 2,$$

од што следува дека $p_i = 2$ за некое i и $\beta_j = \alpha_j$ за $i \neq j$; земајќи да е $p_i = 2$. од (5), се добива

$$(6) \quad 2^{\beta_1 - \alpha_1 - 1} = 2^{\alpha_1 - 1} p_2^{\alpha_2} \dots p_k^{\alpha_k} + 1,$$

т. е. $\alpha_1 = 1$. На тој начин покажавме дека (за $r = 2$) $a \equiv 1 \pmod{2}$ и $a \not\equiv 1 \pmod{4}$, а од тоа следува дека ако $r = 2r'$, тогаш r' е непарен број (бидејќи, поради $a^2 \equiv 1 \pmod{4}$), во спротивен случај не е можно равенството $v(a-1) = v(a^r - 1)$.

Ако q е некој непарен прост број, на ист начин може да се покаже дека равенството $v(a-1) = v(a^q - 1)$ не е можно. Од сето тоа следува точноста на лемата 2.

Сега ќе поминеме на доказот на теоремата.

Нека P_0 е простото потполе од P , т. е. P_0 е полето од класи на остатоци $\text{mod } p$, каде p е карактеристиката на полето P . Ако P_{i-1} е право потполе од P , нека P_i е минималното потполе од P што ги содржи сите елементи од P_{i-1} и еден елемент b_i кој не припаѓа на P_{i-1} ; значи P_i е множеството од сите елементи со облик

$$(7) \quad a_0 + a_1 b_i + \dots + a_{n(b_i)} b_i^{n(b_i)-1},$$

каде $a_0, a_1, \dots, a_{n(b_i)} \in P_{i-1}$.

Јасно е дека секое поле P_i , добиено на тој начин, е конечно, од што следува дека неговата мултипликативна група е циклична. Ако c_i е генератор на таа група, P_i има $n(c_i) + 1$ елементи, па значи постои број s_i така да

$$(8) \quad p^{s_i} = n(c_i) + 1$$

Со оглед на $c_{i-1} \in P_{i-1}$, имаме $n(c_i) \equiv 0 \pmod{n(c_{i-1})}$, т. е.

$$(9) \quad p^{s_i} - 1 \equiv 0 \pmod{p^{s_{i-1}} - 1},$$

од каде, спрема лемата 1, добиваме $s_i \equiv 0 \pmod{s_{i-1}}$, т. е. $s_i = k_i s_{i-1}$, при што $k_i > 1$.

До сега не го користевме условот $v(n(x))$ да е ограничена функција. Претпоставувајќи дека е исполнето и тоа, ќе покажеме дека постои поле P_{i-1} , такво да $P_i = P$; а од тоа ќе следува точноста на теоремата.

Да претпоставиме обратно дека постои бесконечна низа потполиња од P определена на горниот начин, т. е. дека за секое i постои елемент b_i од P што не припаѓа на P_{i-1} . Поради ограниченоста на $v(n(x))$, од тоа следува дека постои природен број l таков да $v(n(c_i)) = v(n(c_{i+j}))$ за секој природен број j . Значи имаме

$$(10) \quad v(n(c_i)) = v(n(c_{i+1})) = v(n(c_{i+2})),$$

т. е.

$$v(p^{s_i} - 1) = v(p^{s_{i+1}} - 1) = v(p^{s_{i+2}} - 1),$$

што, спрема лемата 2, не е можно бидејќи $k_i > 1$. Со тоа е докажана точноста на теоремата.

Како специјален случај на докажаната теорема, земајќи ја во предвид лемата 2, се добива основниот резултат од работата [2].

Познато е дека секој периодичен прстен е комутативен (да се види на пример [1]). Од тоа следува дека појмот периодично тело не содржи ништо ново, бидејќи секое периодично тело е комутативно, т. е. е поле.

ЛИТЕРАТУРА

[1] N. Jacobson, Structure theory for algebraic algebras, Ann. Math. 46, 695—707 (1945).

[2] Г. Чупона, За еден вид полиња со конечна карактеристика, Билтен на Друшт. мат. физ. Макед. 6, 44—46 (1955).

G. Čupona

ON PERIODIC FIELDS

Summary

The field F is said to be periodic if its multiplicative group is periodic¹. Then by $n(x)$ is denoted the multiplicative order of $x (\neq 0)$, and by $\nu(n(x))$ the number of all different prime divisors of $n(x)$.

The purpose of this note is to prove the following result.

Theorem. *The periodic field F is finite if, and only if, $\nu(n(x))$ is bounded.*

Proof. Let p be the characteristic of the periodic field F , and F_0 the prime subfield of F . If F_{t-1} is a proper subfield of F and $b_t \in F \setminus F_{t-1}$, then F_t is the subfield of F which is generated by $F_{t-1} \cup \{b_t\}$, i. e. F_t is the set of all elements

$$(1) \quad a_0 + a_1 b_t + \dots + a_{n(b_t)} b_t^{n(b_t)-1}$$

where $a_0, a_1, \dots, a_{n(b_t)} \in F_{t-1}$.

It is evident that F_t is finite. If c_t is a generator of F_t 's multiplicative group, then F_t contains $n(c_t) + 1$ elements, i. e. there exists s_t such that

$$(2) \quad p^{s_t} - 1 = n(c_t).$$

We have also

$$(3) \quad p^{s_t} - 1 \equiv 0 \pmod{p^{s_{t-1}} - 1}$$

i. e.

$$(4) \quad s_t \equiv 0 \pmod{s_{t-1}}.$$

It can be easily seen that, if $a, r, s > 1$, then

$$(5) \quad v(a-1) = v(a^r-1) \rightarrow v(a^r-1) < v(a^{rs}-1).$$

Therefore, we have

$$(6) \quad v(n(c_{i-1})) = v(n(c_i)) \rightarrow v(n(c_i)) < v(n(c_{i-1}))$$

If we suppose that $v(n(x))$ is bounded, we will obtain that the sequence $F_0, F_1, \dots, F_{i-1}, F_i, \dots$ is finite; then the last member of this sequence is the field F , and so F is finite.

Clearly, if F is finite then $v(n(x))$ is bounded.

¹⁾ It is well known that every periodic division ring is a field too.