ЗА ПЕРИОДИЧНИТЕ ПОЛИЊА

Билтен ДМФ НРМ, Скопје 11 (1960), 5–8

За полето P велиме 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 $\nu(n)$ бројот од сите различни прости делители на n.

Јасно е дека функцијата $\nu(n(x))$ 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 $\nu(n(x))$ е ограничена во периодичното поле P, тогаш тоа поле е конечно.*

При доказот на теоремата ќе ги користиме наредните две леми.

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

(1) $$a^m - 1 \equiv 0 \ (\mathrm{mod}\ a^n - 1) \rightleftarrows m \equiv 0 \ (\mathrm{mod}\ n).$$

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

(2) $$\nu(a-1) = \nu(a^r - 1) \longrightarrow r = 2, \ a \equiv 1 \ (\mathrm{mod}\ 2), \ a \not\equiv 1 \ (\mathrm{mod}\ 4).$$

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

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

каде $m = kn + r$ и $o < r \leqslant n$.

Ќе спомeнеме сега еден начин за докажувањето на втората лема, Нека претпоставиме дека

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

и

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

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

од што следува дека $p_i = 2$ за некое i и $\beta_j = \alpha_j$ за $i \neq j$; земајќи да е $p_1 = 2$. од (5), се добива

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

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

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

Сега ќе поминеме на доказот на теоремата.

Нека $P_\circ$ е простото потполе од P, т. е. $P_\circ$ е полето од класи на остатоци 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_{-1}; значи P_i е множеството од сите елементи со облик

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

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

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

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

(9) $$p^{s_l} - 1 \equiv 0 \pmod{p^{s_{l-1}} - 1},$$

од каде, спрема лемата 1, добиваме $s_l \equiv 0 \pmod{s_{l-1}}$, т. е. $s_l = k_l s_{l-1}$, при што $k_l > 1$.

До сега не го користевме условот $\nu(n(x))$ да е ограничена функција. Претпоставувајќи дека е исполнето и тоа, ќе покажеме дека постои поле P_{l-1}, такво да $P_l = P$, 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 $\nu(n(x))$, од тоа следува дека постои природен број l таков да $\nu(n(c_l)) = \nu(n(c_{l+j}))$ за секој природен број j. Значи имаме

$$\nu(n(c_l)) = \nu(n(c_{l+1})) = \nu(n(c_{l+2})),$$

т. е.

$$\nu(p^{s_l}-1) = \nu(p^{s_l k_{l+1}}-1) = \nu(p^{s_l k_{l+1} k_{l+2}}-1),$$

што, спрема лемата 2, не е можно бидејќи $k_l > 1$. 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] Ѓ. Чупона, За еден вид полиња со конечна карактеристика, Билтен на Друшт. мат. физ. Макед. 6, 44—46 (1955).

ON PERIODIC FIELDS

Summary

The field F is said to be periodic if its multiplicative group is periodic[1]). Then by $n(x)$ is denoted the multiplicative order of x ($\neq 0$), and by $\nu(n(x))$ the number of all differenf 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_{i-1} is a proper subfield of F and $b_i \in F \setminus F_{i-1}$, then F_i is the subfield of F which is generated by $F_{i-1} \cup \{b_i\}$, i. e. F_i is the set of all elements

(1) $$a_0 + a_1 b_i + \cdots + a_{n(b_i)} b^{n(b_i)-1}$$

where $a_0, a_1, \cdots, a_{n(b_i)} \in F_{i-1}$.

It is evident that F_i is finite. If c_i is a generator of its multiplicative group, then F_i contains $n(c_i)+1$ elements, i. e. there exists s_i such that

(2) $$p^{s_i}-1 = n(c_i).$$

We have also

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

i. e.

(4) $$s_i \equiv 0 \pmod{s_{i-1}}.$$

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

(5) $$\nu(a-1) = \nu(a^r-1) \longrightarrow \nu(a^r-1) < \nu(a^{rs}-1).$$

Therefore, we have

(6) $$\nu(n(c_{i-1})) = \nu(n(c_i)) \longrightarrow \nu(n(c_i)) < \nu(n(c_{i-1}))$$

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

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

---

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