УДК 512.6

І. Ю. Раєвська, М. Ю. Раєвська

# МАЙЖЕ–ПОЛЯ З НЕАБЕЛЕВО СПАДКОВИМИ МУЛЬТИПЛІКАТИВНИМИ ГРУПАМИ

I. Yu. Rayevska, M. Yu. Rayevska. *Finite near–fields with hereditary non–abelian groups*, Mat. Stud. **34** (2010), 38–43.

A multiplicative group is said to be hereditary non–abelian if either it is abelian or every its non–abelian subgroup is isomorphic to the multiplicative group of some near–field. A complete classification of hereditary non–abelian groups of finite near–fields is obtained.

И. Ю. Раевская, М. Ю. Раевская. *Почти-поля с неабелево наследственными мультипликативными группами*, Mat. Stud. **34** (2010), 38–43.

Мультипликативная группа почти-поля называется неабелево наследственной, если она абелева, или каждая её абелевая подгруппа изоморфна мультипликативной группе некоторого почти-поля. Получена полная классификация неабелево наследственных мультипликативных групп конечных почти-полей.

**1. Вступ.** В роботі [2] мультиплікативна група майже-поля названа *спадковою*, якщо кожна її підгрупа ізоморфна мультиплікативній групі деякого майже-поля, та наведена повна класифікація таких груп. В даній статті розглядається більш загальне поняття *неабелево спадкової* мультиплікативної групи майже-поля, в якій умова ізоморфізму з мультиплікативними групами майже-полів накладається лише на неабелеві підгрупи.

Нагадаємо, що *майже-полем* називається алгебраїчна структура $F$ з двома операціями, додаванням та множенням, що задовольняє наступним умовам:

1) $F$ утворює абелеву групу відносно додавання, яка називається *адитивною групою* майже-поля $F$ та позначається через $F^+$;

2) множина ненульових елементів $F \setminus 0$ із $F$ утворює групу відносно множення, яка називається *мультиплікативною групою* майже-поля $F$ та позначається через $F^*$;

3) виконується односторонній дистрибутивний закон $a(b+c) = ab + ac$ для всіх $a, b$, $c \in F$.

Очевидно, що кожне тіло є майже-полем. Перші приклади скінченних майже-полів, які не є полями, були наведені Л. Діксоном [1] ще в 1905 році. Найменше з них має порядок 9 та будується наступним чином: визначимо на полі Галуа $F_9 = F(+, \cdot)$ нову операцію $*$ за правилом

$$a * b = \begin{cases} ab, & \text{якщо } a^4 = 1, \\ b^3, & \text{в противному разі.} \end{cases}$$

2000 *Mathematics Subject Classification:* 16N20, 16U60, 20M25.

Прості обчислення показують, що $F = F(+, *)$ є майже-полем, мультиплікативна група $F^*$ якого є групою кватерніонів.

Класифікація скінченних майже-полів була отримана Г. Цассенхаузом [5] в 1936 році. Зокрема, адитивна група $F^+$ кожного такого майже-поля $F$ є елементарною абелевою групою порядку $p^n$ для деякого простого числа $p$ та натурального $n$, а отже порядок його мультиплікативної групи $F^*$ рівний $p^n - 1$. Крім того, згідно з [5, Satz 3] в групі $F^*$ кожна підгрупа порядку $qr$, де $q$ та $r$ — довільні прості дільники числа $p^n - 1$, а тому і кожна абелева підгрупа, є циклічною. Зауважимо також, що основні факти з теорії майже-полів можна знайти в книзі М. Холла [7], глава 20, а детальну інформацію в монографії [4]. Як і в [2], результати нашої статті в значній мірі спираються на деякі елементарні властивості простих дільників числа $p^n - 1$.

**2. Деякі властивості простих чисел.**

Нагадаємо, що просте число $p$, яке має вигляд $p = 2^n - 1$ для деякого натурального $n$, називається простим числом Мерсенна. Як легко бачити, в цьому випадку число $n$ також мусить бути простим. Питання про те, чи існує нескінченна кількість простих чисел Мерсенна, є добре відомою проблемою, яка до сьогоднішнього дня залишається нерозв'язною.

Наступна лема доведена в [2, лема 1].

**Лема 1.** *Нехай $q$ — просте число Мерсенна, $p$ — непарне просте.*

*1) Якщо $m$ і $n$ — додатні цілі числа, тоді з $2^n - 1 = p^m$ випливає $m = 1$ і $n$ — просте.*

*2) $pq + 1 \neq 2^m$ для будь–якого додатного цілого $m$.*

*3) Якщо $r$ — непарне просте і $2p + 1 = r^m$ для деякого додатного $m$, тоді $p = 3$.*

**Означення 1.** Просте число $r$ називається *примітивним простим дільником числа* $p^n - 1$, якщо $r$ ділить $p^n - 1$, але не ділить $p^m - 1$ для кожного $1 \leq m \leq n - 1$.

Критерій існування примітивних простих дільників числа $p^n - 1$ вперше був доведений в [6] і відомий як теорема Жигмонді.

**Теорема 1.** *Для довільного простого числа $p$ та натурального $n > 1$ примітивний простий дільник числа $p^n - 1$ існує, за винятком двох випадків:*

*1) $n = 6$ та $p = 2$; 2) $n = 2$ та $p = 2^s - 1$ — просте число Мерсенна.*

**Лема 2.** *Нехай для деякого натурального $n$ виконується рівність $2^n - 1 = pq^m$, де $p$ та $q$ — прості числа і $m \geq 2$. Якщо $q$ ділить $2^k - 1$ для деякого $k < n$, то $n = 6$, $p = 7$ та $q = 3$.*

*Доведення.* Нехай $k$ — найменше з натуральних чисел, для яких $q$ ділить $2^k - 1$. Тоді $n = kl + r$ для деяких цілих $l, r$ таких, що $0 \leq r < l$. Оскільки

$$2^n - 1 = 2^{kl+r} - 1 = 2^{kl} \cdot 2^r - 2^r + 2^r - 1 = (2^{kl} - 1)2^r + (2^r - 1) =$$
$$= (2^k - 1)(2^{k(l-1)} + \cdots + 2^k + 1)2^r + (2^r - 1) = pq^m$$

та $q$ ділить $2^k - 1$, а отже ділить перший доданок $(2^k - 1)(2^{k(l-1)} + \cdots + 2^k + 1)2^r$, то $q$ мусить ділити другий доданок $2^r - 1$, що в силу вибору числа $k$ можливо лише при $r = 0$. Отже $n = kl$.

Далі, за формулою бінома Ньютона

$$2^n - 1 = (2^k - 1 + 1)^l - 1 = (2^k - 1)^l + \binom{l}{1}(2^k - 1)^{l-1} + \ldots + \binom{l}{l-1}(2^k - 1),$$

звідки

$$(2^k-1)\Big((2^k-1)^{l-1}+\binom{l}{1}(2^k-1)^{l-2}+\ldots+\binom{l}{l-1}\Big)=pq^m. \qquad (*)$$

Припустимо спочатку, що $n\neq 6$. Тоді за теоремою 1 число $p$ є примітивним простим дільником числа $2^n-1$, а отже не ділить $2^k-1$. Але тоді $2^k-1$ ділить $q^m$ і тому $2^k-1=q$ за лемою 1. Таким чином, рівність $(*)$ приймає вигляд $q(q^{l-1}+\binom{l}{1}q^{l-2}+\ldots+\binom{l}{l-1})=pq^m$, звідки $q^{l-1}+\binom{l}{1}q^{l-2}+\ldots+\binom{l}{l-1}=pq^{m-1}$. Це означає, що $q$ ділить $\binom{l}{l-1}=l$, а тому $n=kqr$ для деякого натурального $r$. Отже,

$$2^n-1=2^{kqr}-1=(2^q)^{kr}-1=(2^q-1)(1+2^q+\ldots+2^{(kr-1)q})=pq^m.$$

Оскільки за малою теоремою Ферма $q$ ділить $2^{q-1}-1$, то воно не може ділити $2^q-1$, бо $2^q-1=2^{q-1}+(2^{q-1}-1)$. Отже $p$ мусить ділити $2^q-1$. З іншого боку, $p$ — примітивний простий дільник числа $2^n-1$, а тому може ділити $2^q-1$ лише у випадку $q=n$. Але тоді з рівностей $2^k-1=q=n=kqr$ випливає $q=k=1$, що суперечить умові леми.

Таким чином, $n=6$ і з рівності $2^6-1=7\cdot 3^2$ отримуємо $p=7$ та $q=3$, як стверджувалось. □

**Лема 3.** *Нехай для простих чисел $p$ та $q$ існують такі натуральні числа $n$ та $k$, що $p^n-1=2^kq$. Якщо $k\geq 2$ та $p-1\neq 2^k$, то або $n=2$, $p=5$, 7 та $q=3$, або $n=4$, $p=3$ та $q=5$.*

*Доведення.* Припустимо спочатку, що число $p^n-1$ не має примітивних простих дільників. За теоремою 1 в цьому випадку $n=2$ та $p=2^s-1$ є простим числом Мерсенна. З рівності $2^kq=p^2-1=(2^s-1)^2-1=2^{s+1}(2^{s-1}-1)$ випливає, що $k=s+1$ та $q=2^{s-1}-1$ також є простим числом Мерсенна. Але тоді числа $s$ та $s-1$ є простими за лемою 1 і тому $s=3$. Отже в розглядуваному випадку $n=2$, $p=7$ та $q=3$.

В іншому випадку з рівності $p^n-1=(p-1)(1+p+p^2+\ldots+p^{n-1})=2^kq$ та вказаної теореми випливає, що примітивним простим дільником числа $p^n-1$ є число $q$, а тому $q$ не ділить $p-1$. Тоді $p-1=2^s$ для деякого $s<k$ і отже $2q$ ділить $1+p+p^2+\ldots+p^{n-1}$. Оскільки число $p$ непарне, останнє можливе лише у випадку, коли число $n$ парне, а отже $n=2^lm$ для деякого $l\geq 1$ та непарного числа $m$. Але тоді $q$ як примітивний простий дільник числа $p^n-1$ не ділить число $p^m-1$, а тому з рівності $p^n-1=p^{2^lm}-1=(p^m-1)(1+p^m+\ldots+p^{m(2^l-1)})=2^kq$ випливає, що $p^m-1=2^a$ для деякого числа $a\geq 1$. Оскільки $p^m-1=(p-1)(1+p+\cdots+p^{m-1})$ і число $1+p+\cdots+p^{m-1}$ при непарному $m$ є непарним, рівність $p^m-1=2^a$ можлива лише у випадку $m=1$. Звідси $n=2^l$ і, таким чином, $p^{2^l}-1=2^kq$.

Знову ж таки, оскільки $q$ не ділить $p^{2^{l-1}}-1$, то з рівності $p^{2^l}-1=(p^{2^{l-1}}-1)(p^{2^{l-1}}+1)=2^kq$ випливає, що $p^{2^{l-1}}-1=2^r$ для деякого $r>1$. Але тоді число $p^{2^{l-1}}-1$ не має примітивних простих дільників і тому за теоремою 1 або $2^{l-1}=1$, або $2^{l-1}=2$.

В першому випадку $l=1$, а отже $p^2-1=(p-1)(p+1)=2^kq$. Враховуючи, що $p-1=2^s$, отримуємо $2^s+2=p+1=2^{k-s}q$, звідки $q=2^{s-1}+1$ та $p=2^s+1$. Однак число виду $2^t+1$ може бути простим лише у тому разі, коли $t$ є степенем числа 2, оскільки $x^m+1=(x+1)(x^{m-1}-x^{m-2}+\cdots-x+1)$ при непарному $m$. Звідси $s-1=2^0=1$ та $s=2$, а отже $n=2$, $p=5$ та $q=3$.

В другому випадку $l=2$, $p^4-1=(p^2-1)(p^2+1)=2^kq$ та $p^2-1=2^r$, а тому $p2^s=p(p-1)=p^2-p=2^r-2^s=(2^{r-s}-1)2^s$. Звідси $2^{r-s}-1=p=2^s+1$, що можливо лише при $r=3$ та $s=1$, тобто при $p=3$. З рівності $3^4-1=2^kq$ тепер випливає $q=5$, тобто $n=4$, $p=3$ та $q=5$, що й стверджувалось. □

**3. Мультиплікативна група майже-поля.** Мультиплікативні групи скінченних майже–полів були детально вивчені Цассенхаузом в [5, Satz 17] (див. також М. Холл [7], теорема 20.7.2). Як звичайно, нижче $SL(2,q)$ позначає спеціальну лінійну групу степеня 2 над скінченним полем із $q$ елементів, а $C_n$ — циклічну групу порядку $n$.

**Теорема 2.** *Нехай $F$ — скінченне майже-поле. Тоді його порядок є степенем деякого простого числа, а його мультиплікативна група $F^*$ є або метациклічною групою, або ізоморфною одній з наступних семи груп:*

*I)* $SL(2,3)$; *II)* $SL(2,3)\times C_5$; *III) підгрупа* $O(2,7)$ *порядку* 48 *групи* $SL(2,7)$;
*IV)* $O(2,7)\times C_{11}$; *V)* $SL(2,5)$; *VI)* $SL(2,5)\times C_7$; *VII)* $SL(2,5)\times C_{29}$.

Наступна лема є безпосереднім наслідком твердження 4) теореми 20.7.2 із книги М. Холла [7].

**Лема 4.** *Нехай $F$ — скінченне майже-поле порядку $q^n$ для деякого простого числа $q$ та натурального $n$. Якщо мультиплікативна група $F^*$ цього поля метациклічна і неабелева, то її центр є циклічною підгрупою порядку $q^k-1$ для деякого власного дільника $k$ числа $n$.*

Нагадаємо, що скінченна група називається *групою Міллера–Морено*, якщо вона неабелева, а всі її власні підгрупи є абелевими. Будова таких груп добре відома (див. [3]).

**Лема 5.** *Нехай $G$ — скінченна неабелева група, всі власні підгрупи якої циклічні. Тоді $G$ є або групою кватерніонів порядку* 8, *або напівпрямим добутком $G=\langle a\rangle\rtimes\langle b\rangle$ нормальної підгрупи $\langle a\rangle$ простого порядку $p\neq 2$ з циклічною підгрупою $\langle b\rangle$ порядку $q^n$ для деякого простого дільника $q$ числа $p-1$ та цілого $n\geq 1$, в якому підгрупа $\langle b^q\rangle$ співпадає з центром групи $G$.*

**Лема 6.** *Нехай $F$ — скінченне майже-поле, мультиплікативна група $F^*$ якого є групою Міллера–Морено. Тоді $F^*$ є або групою кватерніонів порядку* 8, *або неабелевою метациклічною групою одного з порядків* 24, 63 *або* 80.

*Доведення.* Оскільки мультиплікативна група кожного скінченного поля є циклічною, майже-поле $F$ не є полем і, зокрема, число його елементів не може бути простим. Тому порядок $F$ рівний $q^n$ для деякого простого числа $q$ та натурального $n>1$, а отже порядок групи $F^*$ рівний $q^n-1$. Враховуючи, що в мультиплікативній групі скінченного майже-поля кожна абелева підгрупа та підгрупа порядку $pr$, де $p$ та $r$ — прості числа, є циклічною, отримуємо, що в групі $F^*$ всі власні підгрупи циклічні і її порядок $q^n-1$ не може бути добутком двох простих чисел. Тому за лемою 5 група $F^*$ є або групою кватерніонів порядку 8, або деякою метациклічною групою порядку $pr^m$, де $p$ — непарне просте число, $r$ — простий дільник числа $p-1$, $m\geq 2$ та підгрупа порядку $r^{m-1}$ співпадає з центром $Z$ групи $F^*$. Оскільки за лемою 4 центр $Z$ є підгрупою порядку $q^k-1$ для деякого власного дільника $k$ числа $n$, то $r^{m-1}=q^k-1$ і для доведення леми залишається встановити, що при цій умові рівність $q^n-1=pr^m$ має місце лише у випадках, коли $n=2$ та $q=5$, $n=4$ та $q=3$ або $n=6$ та $q=2$.

Припустимо спочатку, що $q=2$. Тоді $2^n-1=pr^m$ та $r^{m-1}=2^k-1$, де $k$ — власний дільник числа $n$. Оскільки $m\geq 2$, то $r$ ділить $2^k-1$ і тому за лемою 2 маємо $n=6$.

Нехай тепер $q\neq 2$. Тоді число $q^n-1$ парне, а тому $r=2$. Отже $q^n-1=2^mp$ та $2^{m-1}=q^k-1$. Звідси $q-1\neq 2^m$ і тому, застосовуючи лему 3, отримуємо $n=2$ та $q=5$ або $n=4$ та $q=3$, що й вимагалося. □

**Лема 7.** *Нехай $F$ — скінченне майже-поле, мультиплікативна група $F^*$ якого є метациклічною. Тоді $F^*$ не містить підгрупи простого індексу, яка є групою Міллера–Морено, ізоморфною мультиплікативній групі деякого майже-поля.*

*Доведення.* Припустимо протилежне, і нехай $H$ — підгрупа Міллера–Морено простого індексу $p$ в $F^*$, яка ізоморфна мультиплікативній групі деякого майже-поля. Тоді за лемою 6 порядок $h$ підгрупи $H$ є одним із чисел 8, 24, 63 або 80. Оскільки порядок майже-поля $F$ рівний $q^n$ для деякого простого числа $q$ та цілого $n > 1$, то порядок групи $F^*$ задовольняє співвідношення $hp = q^n - 1$. Зрозуміло також, що або центр $Z$ групи $F^*$ міститься в $H$, а отже і в центрі підгрупи $H$, або $F^* = HZ$. Отже, якщо $z$ — порядок центру $Z$, то в першому випадку за лемою 5 $z$ ділить, відповідно, одне із чисел 2, 4, 3 або 8, а в другому $z$ ділиться на $p$. Крім того, за лемою 4 $z = q^k - 1$ для деякого власного дільника $k$ числа $n$. Розглянемо спочатку випадок, коли $Z$ міститься в $H$.

Якщо $h = 8$, то $z = 2$ і тому $q = 3$. Тоді з рівності $8p = 3^n - 1$ випливає, що $n = 2m$ для деякого $m > 1$, звідки $8p = (3^m - 1)(3^m + 1)$. Оскільки $p$ є примітивним простим дільником числа $3^n - 1$ за теоремою 1, то $p$ не ділить $3^m - 1$ і тому $3^m - 1$ ділить 8. Але тоді $m = 2$, а отже $p = 10$, всупереч тому, що $p$ — просте число.

Нехай $h = 24$. Тоді $z = q^k - 1$ ділить 4 і тому $q = 3$ або $q = 5$. В першому випадку, однак, рівність $24p = 3^n - 1$ неможлива, а тому $q = 5$. Тоді з рівності $24p = (5^2 - 1)p = 5^n - 1$ знову виводимо, що $n = 2m$ для $m > 1$. Звідси $24p = (5^m - 1)(5^m + 1)$ та $p$ не ділить $5^m - 1$. Отже $5^m - 1$ ділить 24, звідки $m = 2$ та $p = 26$, що суперечить простоті числа $p$.

Далі, якщо $h = 63$, то $z = q^k - 1$ ділить 3 і тому $q = 2$. Тоді з рівності $63p = (2^6 - 1)p = 2^n - 1$ випливає, що $n = 6m$ для $m > 1$, звідки $63p = (2^{3m} - 1)(2^{3m} + 1)$. За теоремою 1 число $p$ є примітивним простим дільником числа $2^n - 1$ і тому не ділить $2^{3m} - 1$. Звідси $2^{3m} - 1$ ділить 63 і, таким чином, $m = 2$ та $p = 65$, що знову суперечить простоті числа $p$.

Нарешті, якщо $h = 80$, то $z = q^k - 1$ ділить 8 і тому $q = 3$ або $q = 5$. Оскільки в останньому випадку рівність $80p = 5^n - 1$ неможлива, то $q = 3$ і тому $80p = (3^4 - 1)p = 3^n - 1$. Звідси та теореми 1 отримуємо, що $n = 4m$ для $m > 1$ та $p$ не ділить $3^{2m} - 1$. Але тоді $3^{2m} - 1$ ділить 80 і тому $m = 2$ та $p = 82$, що знову ж таки неможливо.

Таким чином, центр $Z$ не міститься в $H$ і, отже, $F^* = HZ$. Очевидно, тоді перетин $H \cap Z$ співпадає з центром підгрупи $H$, а тому порядок центру $Z$ рівний $z = 2p$ при $h = 8$, $z = 4p$ при $h = 24$, $z = 3p$ при $h = 63$ та $z = 8p$ при $h = 80$. Оскільки порядок групи $F^*$ рівний $hp$, то порядок фактор–групи $F^*/Z$ рівний, відповідно, одному із чисел 4, 6, 21 або 10. З іншого боку, порядок $F^*$ рівний $q^n - 1$ та $z = q^k - 1$, де $n = mk$ для деякого $k \geq 1$, тобто порядком $F^*/Z$ є число $\frac{q^n-1}{q^k-1} = 1 + q^k + \cdots + q^{k(m-1)}$.

Отже, якщо $q^k - 1 = z = 2p$, то $4 = 1 + q^k + \cdots + q^{k(m-1)}$, звідки $k = 1$ та $q = 3$. Але тоді $p = 1$, що суперечить припущенню леми. Далі, якщо $q^k - 1 = z = 4p$, то $6 = 1 + q^k + \cdots + q^{k(m-1)}$, звідки $k = 1$ та $q = 5$, що теж неможливо, бо тоді теж $p = 1$. Очевидно також, що при $q^k - 1 = z = 3p$ рівність $21 = 1 + q^k + \cdots + q^{k(m-1)}$ неможлива, а при $q^k - 1 = z = 8p$ з рівності $10 = 1 + q^k + \cdots + q^{k(m-1)}$ випливає $k = 2$ та $q = 3$, звідки знову $p = 1$. Останнє протиріччя завершує доведення леми. □

**Теорема 3.** *Нехай $F$ — скінченне майже-поле, мультиплікативна група $F^*$ якого є неабелево спадковою. Тоді $F^*$ — група одного з наступних типів:*

*1) циклічна група; 2) група кватерніонів $Q_8$;*

*3) неабелева метациклічна група порядку 24; 4) група $SL(2, 3)$;*

*5) неабелева метациклічна група порядку* 63*;*

*6) неабелева метациклічна група порядку* 80*;*

*Доведення.* Якщо група $F^*$ абелева, то вона циклічна, тобто типу 1), оскільки в цьому випадку $F$ є полем. Нехай далі $F^*$ є неабелевою групою. Тоді вона містить деяку неабелеву підгрупу $H$, що є групою Міллера–Морено. Оскільки за умовою теореми $H$ ізоморфна мультиплікативній групі деякого майже-поля, то за лемою 6 вона є або групою кватерніонів порядку 8, або неабелевою метациклічною групою одного з порядків 24, 63 або 80. Отже, якщо $F^* = H$, то $F^*$ є групою одного з типів 2), 3), 5) або 6). Більш того, якщо група $F^*$ метациклічна і $H$ її власна підгрупа, то $H$ мусить бути підгрупою простого індексу в деякій неабелевій підгрупі із $F^*$, що за лемою 7 неможливо, оскільки остання теж ізоморфна мультиплікативній групі деякого майже-поля. Отже, неабелево спадкова метациклічна група $F^*$ є групою одного з вказаних вище типів.

Припустимо тепер, що група $F^*$ неметациклічна. Тоді вона є однією з груп I)–VII) теореми 2. У випадку I) $F^*$ ізоморфна групі $SL(2,3)$ і тому її єдиною власною неабелевою підгрупою є підгрупа, що ізоморфна група кватерніонів $Q_8$. Отже в цьому випадку $F^*$ є неабелево спадковою групою типу 4). У випадку II) група $F^*$ не є неабелево спадковою, бо вона містить підгрупу порядку 40, ізоморфну групі $Q_8 \times C_5$, яка не може бути мультиплікативною групою майже-поля, оскільки 40 не є числом виду $q^n - 1$ при $n \geq 2$. У випадку III) група $F^*$ теж не є неабелево спадковою, бо вона містить підгрупу порядку 16, яка ізоморфна узагальненій групі кватерніонів $Q_{16}$, і тому також не може бути мультиплікативною групою майже-поля. З цієї ж причини $F^*$ не є неабелево спадковою групою і у випадку IV). Нарешті, група $SL(2,5)$, а отже групи V)–VII), не є неабелево спадковими, оскільки в $SL(2,5)$ міститься неабелева підгрупа порядку 10, яка не є мультиплікативною групою майже-поля. Отже групами типів 1)–6) вичерпуються всі неабелево спадкові мултиплікативні групи скінченних майже-полів. □

## ЛІТЕРАТУРА


1. L.E. Dixon, *Definitions of a group and a field by independent postulates*, Trans. Amer. Math. Soc. **6** (1905), 198–204.
2. S. Ligh, *Finite Hereditary Near-field groups*, Mh. Math. **86** (1978), 7-11.
3. G.A. Miller, H. Moreno, *Non-abelian groups in which every subgroup is abelian*, Trans. Amer. Math. Soc. **4** (1903), 398-404.
4. H. Wahling, Theorie der Fastkörper, Essen: Thales Verlag, 1987.
5. H. Zassenhaus, *Über endliche Fastkörper*, Ab. Math. Sem. Univ. Hamburg, **11** (1935/36), 187-220.
6. K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys., **3** (1892), 265–284.
7. М. Холл, Теория групп, М.: Издательство иностранной литературы, 1962, 468 с.



Інститут математики НАН України,
raemarina@rambler.ru



*Надійшло 16.02.2010*
*Після переробки 14.09.2010*