Визначимо множення * в G таким чином, щоб $(G,+,*)$ було локальним майже-кільцем. Для кожного $x, y \in G$ покладемо

$$x*y=(x*a)y_1+(x*b)y_2+(x*c)y_3=a(x_1y_1+y_2\alpha(x))+b(x_2y_1+y_2\beta(x))+c\left(x_1y_3\beta(x)+x_3y_1+y_2\gamma(x)-x_1x_2\binom{y_1}{2}\right),$$

причому відображення $\alpha: R\to Z_{p^m}$, $\beta: R\to Z_{p^n}$, $\gamma: R\to Z_p$, задовольняють умовам:

1) $\alpha(x*y)=x_1\alpha(y)+\alpha(x)\beta(y)$,
2) $\beta(x*y)=x_2\alpha(y)+\beta(x)\beta(y)$,
3) $\gamma(x*y)=\beta(y)\gamma(x)+x_1\beta(x)\gamma(y)$,
4) $x_1\neq 0(\mathrm{mod}\ p)\Rightarrow\beta(x)\neq 0(\mathrm{mod}\ p)$.

Покажемо, що $(G,+,*)$ є локальним майже-кільцем.

Лема 5. $(G,*)$ є напівгрупою.

Лема 6. Операція * є ліво дистрибутивною відносно операції + ($x*(y+z)=x*y+x*z$).

Очевидно, що $e=(1,0,0)$ є мультиплікативною одиницею. З лем 5 та 6 випливає доведення наступної теореми.

Теорема 5. $R\cong(G,+,*)$ є майже-кільцем з одиницею.

Так як $(G,+)$ є неабелева група, то R не є кільцем.

Лема 7. $k=ak_1+bk_2+ck_3\in L$, тоді і тільки тоді, коли $k_1\equiv 0\ (\mathrm{mod}\ p)$.

Таким чином, доведено наступну теорему.

Теорема 6. $R\cong(G,+,*)$ є локальним майже-кільцем.

Зокрема, можуть бути такі значення функцій $\alpha(x)=\gamma(x)=0$ і $\beta(x)=x_1$. Легко бачити, що вони задовольняють умови (1) – (4) і як наслідок маємо наступну теорему.

Теорема 7. Якщо відображення $\alpha: R\to Z_{p^m}$, $\beta: R\to Z_{p^n}$, $\gamma: R\to Z_p$, задовольняють умови $\alpha(x)=\gamma(x)=0$ і $\beta(x)=x_1$ для кожного $x\in G$, то операція

$$x*y=(x*a)y_1+(x*b)y_2+(x*c)y_3=a(x_1y_1+y_2\alpha(x))+b(x_2y_1+y_2\beta(x))+c\left(x_1y_3\beta(x)+x_3y_1+y_2\gamma(x)-x_1x_2\binom{y_1}{2}\right)$$

на адитивній групі G є асоціативною та ліво-дистрибутивною і визначає деяке нуль-симетричне локальне майже-кільце $R=(G,+,*)$.

5. Висновки

Доведено необхідні та достатні умови існування локальних майже-кілець на неметациклічній p-групі Міллера-Морено.

1. *Левищенко С.С., Кузенный Н.Ф.* Группы с условиями дисперсивности для подгрупп. – Киев: КГПИ, 1985. – 96 с. 2. *Холл М.* Теория групп. – М.: Издательство иностранной литературы, 1962. – 468 с. 3. *Maxson C.J.* Local near-rings of cardinality p^2 // Canad. Math. Bull. – 1968. – Vol. 11, No. 4. 4. *Maxon C.J.* On local near-rings // Math. Z., 106. – P. 197–205, 1968. 5. *Maxson C.J.* On the construction of finite local near-rings (I): on non-cyclic abelian p-groups // Quart. J. Math. Oxford (2), 21 (1970). – P. 449–457. 6. *Maxson C.J.* On the construction of finite local near-rings (II): on non-abelian p-groups // Quart. J. Math. Oxford (2), 22 (1971). – P. 65–72.

Надійшла до редколегії 20.12.2010 р.

УДК 512.6

М. Раєвська, асп.

ЛОКАЛЬНІ МАЙЖЕ-КІЛЬЦЯ З МУЛЬТИПЛІКАТИВНОЮ ГРУПОЮ МІЛЛЕРА-МОРЕНО

Описано всі майже-поля з мультиплікативною групою Шмідта та вивчено локальні майже-кільця з мультиплікативною групою Міллера-Морено, що не є 2-групою.

All near-fields with multiplicative Schmidt group are described. Furthermore, local near-rings with multiplicative Miller-Moreno group which is not a 2-group are studied.

1. Вступ

Алгебраїчна структура R з двома бінарними операціями + і $\cdot$ називається (лівим) майже-кільцем, якщо $(R,+)$ – необов'язково абелева група, $(R,\cdot)$ – напівгрупа та $r(s+t)=rs+rt$ для всіх $r, s, t\in R$. Група $(R,+)$ позначається через R^+ та називається адитивною групою, а її нейтральний елемент 0 – нулем майже-кільця R. Група всіх оборотних елементів напівгрупи $(R,\cdot)$ називається мультиплікативною групою в R та позначається через R^*. Майже-кільце R з одиницею називається локальним, якщо множина L всіх необоротних елементів із $(R,\cdot)$ утворює адитивну підгрупу в R^+, і майже-полем, якщо $L=0$. Нормальна підгрупа I групи R^+ називається ідеалом (лівого) майже-кільця R, якщо для довільних елементів $r, s\in R$ та $a\in A$ виконуються включення $ra\in I$ та $(r+a)s-rs\in I$. Якщо I – ідеал в R, то фактор-група R/I утворює майже-кільце, яке є узагальненням поняття фактор-кільця [5].

В [2] описано неабелево спадкові мультиплікативні групи скінченних майже-полів. Мультиплікативна група майже-поля називається неабелево спадковою, якщо вона або абелева, або кожна її неабелева підгрупа ізоморфна мультиплікативній групі деякого майже-поля. У даній статті описано всі майже-поля з мультиплікативною групою Шмідта. Також вивчено локальні майже-кільця з мультиплікативною групою Міллера-Морено з індексом $|R:L|\neq 2$. Як і в [4], результати нашої статті спираються на деякі елементарні властивості простих дільників числа p^n-1.

2. Попередні результати

Нагадаємо, що просте число p, яке має вигляд $p=2^n-1$ для деякого натурального n, називається простим числом Мерсенна.

Теорема 1 [4]. Нехай q – просте число Мерсенна, p – непарне просте.

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

$pq+1=2^m$ для будь-якого додатного цілого m.

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 $1\le m\le n-1$.

Наступна теорема встановлює критерій існування примітивних простих дільників числа p^n-1.

Теорема 2 [7]. Для довільного простого числа p та натурального $n>1$ примітивний простий дільник числа p^n-1 існує, за винятком двох випадків:

1) $p=2,\ n=6;$

2) $p=2^t-1,\ n=2.$

Лема 1 [2]. Нехай для деякого натурального s виконується рівність $2^s-1=qr^m,$ де q та r – прості числа і $m>2$. Якщо r ділить 2^k-1 для деякого $k<s$, то $s=6$, $q=7$ та $r=3.$

Лема 2 [2]. Нехай для простих чисел p та q існують такі натуральні числа s та k, що $p^s-1=2^k q.$ Якщо $k>2$ та $p-1=2^k$, то або $s=2,\ p=5,\ 7$ та $q=3$, або $s=4$, $p=3$ та $q=5$.

Означення 2. Скінченна група називається групою Міллера-Морено, якщо вона неабелева, а всі її власні підгрупи є абелевими.

Теорема 3 [1]. Групи Міллера-Морено вичерпуються групами наступних типів:

1) група кватерніонів Q_8;

2) $G=<a>\leftthreetimes<b>,\ |a|=p^m,\ |b|=p^n,\ m\neq 2,\ n\neq 1,\ b^{-1}ab=a^{1+p^{m-1}}$;

3) $G=(<c>\times<a>)\leftthreetimes<b>,\ |c|=p,\ |b|=p^n,\ |a|=p^m,\ m\neq 1,\ n\neq 1,\ b^{-1}ab=ac,\ b^{-1}cb=c$;

4) $G=P\leftthreetimes Q,\ Q=\langle b\rangle$ та $|Q|=q^k,\ \langle b^q\rangle=Z(G),\ Q\lhd G,\ P$ – мінімальний нормальний дільник групи G порядку r^s, де q та r – прості числа.

Означення 3. Групою Шмідта (або мінімальною ненільпотентною) називається скінченна ненільпотентна група, будь-яка власна підгрупа якої нільпотентна.

Теорема 4 [1]. Скінченна група G тоді і лише тоді являється групою Шмідта, коли вона розкладається в напівпрямий добуток $G=S\leftthreetimes T$ своїх нормальної силовської s-підгрупи S порядку s^α, $\alpha\ge 1$, та ненормальної силовської t-підгрупи $\mathrm{T}=\langle \mathrm{b}\rangle$ порядку t^β, $\beta\ge 1$, та задовольняє наступні умови:

$Z(G)=\Phi(G)=\Phi(S)\times\langle b^t\rangle,$ де $\Phi(G)$ – підгрупа Фраттіні групи G;

$G'=S,\ S'=\Phi(S),\ G''=S'$ експонента S' неперевищує число s;

Якщо S – неабелева, то $Z(S)=S'=\Phi(S)$.

Лема 3. Нехай $G\cong A\leftthreetimes\langle b\rangle,\ |A|=p^n,\ p$ – просте число та $p>2,\ |\langle b\rangle|=2^k,\ \langle b^2\rangle=Z(G),\ A$ – мінімальна нормальна підгрупа в G. Тоді $|A|=p.$

Доведення. Нехай $\langle a\rangle$ підгрупа простого порядку в A. Візьмемо елемент $x=ab^{-1}ab=aa^b\in A$. Оскільки $a^{b^2}=a$ і підгрупа A – абелева, то $x^b=\left(aa^b\right)^b=a^ba^{b^2}=a^ba=aa^b=x.$ Можливі два випадки: $x=1$ та $x\neq 1$. Якщо $x=1$, то $aa^b=1$ та $a^b=a^{-1}$. Звідси $\langle a\rangle^b=\langle a\rangle$, тобто $\langle a\rangle$ – нормальна підгрупа. З того, що A мінімальна нормальна підгрупа в G випливає, що $A\cong\langle a\rangle$. Якщо $x\neq 1$, то підгрупа породжена елементом $\langle x\rangle$ є нормальною. Оскільки A мінімальна нормальна, то $A\cong\langle x\rangle$. Отже, порядок A дорівнює p.

3. Майже-поля з мультиплікативною групою Шмідта

Класифікація скінченних майже-полів отримана Г. Цассенхаузом [8] 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 [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 [3], глава 20, а детальну інформацію – в монографії [6].

Лема 4 [3]. Силовська підгрупа групи M непарного порядку циклічна. Силовська 2-підгрупа групи M циклічна або ж являється узагальненою групою кватерніонів. (M – група ізоморфна мультиплікативній групі майже-поля).

Приймемо наступні позначення: F – майже-поле, F^* його мультиплікативна група, F^+ – адитивна група майже-поля, $SL(n,m)$ – спеціальна лінійна група степеня n над скінченним полем із m елементів, C_k – циклічна група порядку k.

Теорема 5 [3]. 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:

1) $SL(2,3)$;
2) $SL(2,3)\times C_5$;
3) підгрупа $O(2,7)$ порядку 48 групи $SL(2,7)$;
4) $O(2,7)\times C_{11}$;
5) $SL(2,5)$;
6) $SL(2,5)\times C_7$;
7) $SL(2,5)\times C_{29}$.

Наступна лема є безпосереднім наслідком твердження 4) теореми 20.7.2 із книги М. Холла [3].

Лема 5. Нехай F – скінченне майже-поле порядку p^s для деякого простого числа p та натурального s. Якщо мультиплікативна група F^* цього поля метациклічна і неабелева, то її центр є циклічною підгрупою порядку p^k-1 для деякого власного дільника k числа s.

Лема 6 [2]. 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 $n>1$, в якому підгрупа $\langle b^q\rangle$ співпадає з центром групи G.

Теорема 6. Нехай F – скінченне майже-поле порядку p^s, мультиплікативна група F^* якого є групою Шмідта. Тоді F^* – група одного з наступних типів:

1) група $SL(2,3)$;
2) неабелева метациклічна група одного з порядків 24, 63, 80.

Доведення. Оскільки порядок F рівний p^s, то порядок групи F^* рівний p^s-1. За теоремою 4 $F^*=P\rtimes\langle b\rangle$, де P є силовською q-підгрупою групи F^* порядку q^n, $|b|=t^m$, $b^t\in Z(F^*)$, $(q,t)=1$. За лемою 4 підгрупа P або циклічна, або узагальнена група кватерніонів.

Нехай P – узагальнена група кватерніонів порядку не менше 16. Оскільки група автоморфізмів такої групи є 2-групою, то $F^*=P\times\langle b\rangle$. Але тоді група F^* буде нільпотентною, що суперечить умові теореми. Отже P або циклічна, або група кватерніонів Q_8.

У випадку, коли $P\cong Q_8$, мультиплікативна група майже-поля F^* ізоморфна групі $SL(2,3)$ за теоремою 5.

Якщо P є циклічною, то F^* – неабелева метациклічна група. Враховуючи, що в мультиплікативній групі скінченного майже-поля кожна абелева підгрупа та підгрупа порядку qr, де r – просте число, є циклічною, отримуємо, що в групі F^* всі власні підгрупи циклічні і її порядок p^s-1 не може бути добутком двох простих чисел. Тому за лемою 6 група F^* є деякою метациклічною групою порядку qr^m, де q – 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 5 центр Z є підгрупою порядку p^k-1 для деякого власного дільника k числа s, то $r^{m-1}=p^k-1$ і для доведення леми залишається встановити, що при цій умові рівність $p^s-1=qr^m$ має місце лише у випадках, коли $s=2$ та $p=5$, $s=4$ та $p=3$ або $s=6$ та $p=2$.

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

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

Отже, F^* – неабелева метациклічна група одного з порядків 24, 63 або 80.

4. Локальні майже-кільця з мультиплікативною групою Міллера-Морено

Нехай R – скінченне локальне майже-кільце порядку p^n, мультиплікативна група R^* якого є групою Міллера-Морено. Підгрупу всіх необоротних елементів із R будемо позначати через L. Тоді L – ідеал в R та $L+1$ – нормальна підгрупа в R^*.

Оскільки R^+ являється p-групою, то $|L| = p^m$, для деякого $m < n$. Фактор-група R/L ізоморфна адитивній групі майже-поля F та мультиплікативна група $(R/L)^* = R^*/L+1$ майже-кільця R/L ізоморфна мультиплікативній групі майже-поля F^* [5]. Оскільки $R = R^* \cup L$ та $R^* \cap L = \varnothing$, то $|R| = |R^*| + |L|$. Звідси випливає, що $|R^*| = p^n - p^m = p^m(p^{n-m} - 1)$. Отже, група $L+1$ має в R^* доповнення K за лемою Шура, а тому мультиплікативна група R^* розкладається у напівпрямий добуток $R^* = (1+L) \rtimes K$, де $K \cong (R/L)^*$. За теоремою 3 $1+L$ є мінімальною нормальною підгрупою в R^* та порядок $|K| = q^k$, де q - деяке просте число.

Лема 7. Нехай R – локальне майже-кільце порядку p^n ($n > 2$), підгрупа L якого циклічна та нетривіальна. Тоді група R^+ – циклічна та порядок L дорівнює p^{n-1}. Крім того, $R^* \cong C_{p^{n-1}} \rtimes C_{p-1}$.

Нехай x належить L і r елемент із R. Тоді відображення $\hat{x} : r \to xr$ являється ендоморфізмом групи R^+, оскільки $x(r_1 + r_2) = xr_1 + xr_2$. Оскільки, ядро ендоморфізму $Ker\,\hat{x} = \{r \in R \mid xr = 0\}$ співпадає з анулятором елемента x в R, то $R^+/Ann_R(x) \cong xR$, де xR лежить в L. З того, що анулятор $Ann_R(x)$ є правим ідеалом в R і не містить 1 випливає, що $Ann_R(x) \leq L$. З циклічності L випливає, що $Ann_R(x)$ та $\mathrm{Im}\,\hat{x}$ є циклічні підгрупи в R^+, а тому R^+ – метациклічна. З того, що $R^+/L \cong \left(R^+/Ann_R(x)\right)/\left(L/Ann_R(x)\right)$ і фактор-група R^+/L є елементарною абелевою випливає, що індекс підгрупи L в R^+ дорівнює p. Згідно [3,теорема 12.5.1] існують сім груп, які мають циклічну підгрупу індексу p. У шести з цих груп, крім циклічної, множина $R^+ \setminus L$ містить елементи порядку p. З іншого боку, в локальному майже-кільці R порядок кожного елемента цієї множини дорівнює експоненті адитивної групи R^+. Отже, адитивна група локального майже кільця R^+ – циклічна.

Лема 8. Нехай R – локальне майже-кільце порядку p^n з $n > 2$ та $p > 2$. Тоді p – просте число Ферма, $R^+ \cong C_p \times C_p$ або $R^+ \cong C_{p^2}$, $|L| = p$ та $R^* \cong C_p \rtimes C_{p-1}$.

Лема 9. Нехай R – локальне майже-кільце порядку 2^n ($n > 2$). Якщо $|R : L| \neq 2$, то L – елементарна абелева 2-група та R^+ - 2-група експоненти не вище 4.

З лем 8, 9 та [2] випливає наступна теорема.

Теорема 7. Нехай R – локальне майже-кільце порядку p^n ($n > 2$), мультиплікативна група якого є групою Міллера-Морено та L підгрупа всіх необоротних елементів з R. Тоді виконуються наступні твердження:

1) якщо R – майже-поле, то R^* є або групою кватерніонів Q_8, або неабелевою метациклічною групою одного з порядків 24, 63, 80;

2) якщо $p > 2$, то p – просте число Ферма, $R^+ \cong C_p \times C_p$ або $R^+ \cong C_{p^2}$, $|L| = p$ та $R^* \cong C_p \rtimes C_{p-1}$;

3) якщо $p = 2$ та індекс $|R : L| \neq 2$, то L – елементарна абелева 2-група та R^+ - 2-група експоненти не вище 4.

5. Висновки

Описано всі майже-поля з мультиплікативною групою Шмідта та вивчено локальні майже-кільця з мультиплікативною групою Міллера-Морено з індексом групи необоротних елементів в адитивній групі локального майже-кільця нерівним 4.

1. *Левищенко С.С., Кузенный Н.Ф.* Группы с условиями дисперсивности для подгрупп. – Киев: КГПИ, 1985. – 96 с. 2. *Раєвська І.Ю., Раєвська М.Ю.* Майже-поля з неабелево спадковими мультиплікативними групами // Мат. Студ. – 2010. – № 34. 3. *Холл М.* Теория групп. – М.: Издательство иностранной литературы, 1962. – 468 с. 4. *Ligh S.* Finte Hereditary Near-field groups / Ed. H.W. Engl // Mh. Math. – 86, 1978. – P. 7–11. 5. *Sysak Ya.P.*Products of groups and local nearrings // Note di Mat. 28 (2008), N. 2. – P. 177–211. 6. *Wahling H.*Theorie der Faztkorper. – Essen:Thales Verlag, 1987. 7. *Zsigmondy K.* Zur Theorie der Potenzreste // Monatsh. Math. Phys., 1892. – Bd 3. – S. 265–284. 8. *Zassenhaus H.* Ueber endliche Fastkoerper // Ab. Math. Sem. Univ. – Hamburg, 11 (1935/1936). – S. 187–220.

Надійшла до редколегії 21.12.2010 р.