FILOMAT (Niš) 9:3 (1995), 867–872
Algebra, Logic & Discrete Mathematics
Niš, April 14–16, 1995.

ON MODIFICATIONS OF THE GALOIS GROUP

Boris V. Novikov

ABSTRACT. In this paper we define Doss modifications of groups and we describe such modifications of a simple cyclic group.

Let K be a field, L a finite normal extension of K with the Galois group G. Sweedler [4] has defined a Brauer monoid $M(G, L)$ which allows to classify so called strongly primary algebras. $M(G, L)$ is a semilattice of Abelian groups and its idempotents are in $1-1$ correspondence with some of partial orders on G (so called lower subtractive G-posets).

Another approach to studying the structure of the Brauer monoid was suggested in [3]. Let 0 be an element not contained in a finite multiplicative group G. We call *a modification* of G the monoid on $G \cup \{0\}$ with an operation $*$ such that $x * y$ is equal to xy or 0 for $x, y \in G$, and besides $1 * x = x * 1 = x, 0 * 0 = 0 * x = x * 0 = 0$. It was shown in [3] that there exists a $1-1$ correspondence between the modifications of G and the idempotents of $M(G, L)$. Moreover, the describing of a Brauer monoid may be reduced to the studying of the modifications because their second 0-cohomology groups [2] are isomorphic to the group components of $M(G, L)$.

However, the enumerating of all modifications of a given group seems to be a difficult problem. In the general case there are known simple properties of modifications only such as [3]:

a) the modifications yields the condition of 0-cancellativity: if $x * z = y * z \neq 0$ or $z * x = z * y \neq 0$ then $x = y$;
b) the ideal of all non-invertible elements of a modification is nilpotent.

In this paper we describe a kind of modifications of a simple cyclic group.

Definition. The modification S of a group G is called *a Doss modification* (analogously to the well-known condition for embedding a semigroup into a group [1]) if

$$(\forall a, b \in S) \quad a * S \cap b * S \neq 0 \Rightarrow a \in b * S \ \vee \ b \in a * S.$$

In what follows we assume that $G = \langle a | a^p = 1 \rangle$ is a cyclic group of prime order p, S is its commutative Doss modification, different from $G^0(.)$ (i.e. $\exists x, y \in G \quad x * y = 0$).

Lemma 1. *S is a 0-direct union of monogenic semigroups (which are generated by indecomposable elements) with joined identity.*

Proof. If x, y are indecomposable elements then $x*S \cap y*S = 0$; in particular, $\langle x \rangle * \langle y \rangle = \langle y \rangle * \langle x \rangle = 0$. Since G has the prime order the subgroup of invertible elements is trivial. So every nonidentity element of S is divided by an indecomposable element and is in fact a power of it. Therefore $S - \{1\}$ is 0-direct union of the monogenic subsemigroups generated by the indecomposable elements. □

Remark. Evidently, the converse assertion is true too.

We shall describe the commutative Doss modifications with two or three generators. It will conveniently to denote an element $a^k \in G$ by b_k, when it is regarded as an element of S (hence $b_k^n = a^k * \cdots * a^k$ n times). Accordingly to Lemma 1 $T = S - \{1\}$ is a semigroup which has the presentation of the form

$$T = \langle b_{i_1}, \ldots, b_{i_r} | b_{i_k}^{\alpha_k} = 0, 1 \leq k \leq r \rangle$$

whence $\alpha_1 + \cdots + \alpha_r = p + r - 1$.

Theorem 1. *If $r = 2$ then*

$$T = \left\langle b_k, b_{p-k} | b_k^m = b_{p-k}^{p-m+1} = 0 \right\rangle$$

where $1 \leq k \leq p-1, 2 \leq m \leq p-1$.

Proof. Let

$$T = \left\langle b_k, b_l | b_k^m = b_l^{p-m+1} = 0 \right\rangle$$

for some $1 \leq k, l \leq p-1, k \neq l$. We may assume that $k < l$. Since

$$\{b_k, b_k^2, \ldots, b_k^{m-1}, b_l, b_l^2, \ldots, b_l^{p-m}\} = \{a, a^2, \ldots, a^{p-1}\}$$

we obtain, regarding b_i^j as the element $a^{ij} \in G$:

$$k + 2k + \cdots + (m-1)k + l + 2l + \cdots + (p-m)l \equiv 1 + 2 + \cdots + (p-1) \pmod{p}$$

or

$$m(m-1)k + m(m-1)l \equiv 0 \pmod{p}.$$

Therefore $k + l \equiv 0 \pmod{p}$ because $2 \leq m \leq p-1$. □

Corollary. *The number of all distinct (but maybe isomorphic) 2-generated commutative Doss modifications is equal* $(p-1)(p-2)/2$.

The situation for $r = 3$ is more complicated. We need a number-theoretic lemma:

Lemma 2. *Let* k, α, x *be integers,* $\frac{p+2}{3} \leq \alpha \leq x \leq p-3$. *Denote the residue* $kx (mod\ p)$ *by* ρ_k *(i.e.* $0 \leq \rho_k \leq p-1$). *If* $\rho_k \geq \alpha$ *for all* $1 \leq k \leq (p-\alpha)/2$ *then* $p \equiv 1 (mod\ 3), a = (p+2)/3$ *and* $x = (p-1)/2$.

Proof. If $x \neq (p-1)/2$ then either $x \leq (p-3)/2$ or $x \geq (p+1)/2$. So we consider three cases.

1. Let $x \leq (p-3)/2$ (then $(p+2)/3 \leq (p-3)/2$ whence $p \geq 13$).

We shall prove by induction by i that if $r_1, r_3, \ldots, r_{2i-1} \geq (p+2)/3$ then $\rho_{2i+1} = (2i+1)x - ip$.

For $i = 0$ it is evidently. Let

$$\rho_{2i-1} = (2i-1)x - (i-1)p \geq (p+2)/3.$$

Then

$$(2i+1)x - ip = \rho_{2i-1} + 2x - p \geq 0,$$

$$(2i+1)x - (i+1)p = \rho_{2i-1} + 2x - 2p < p + (p-3) - 2p < 0$$

and

$$\rho_{2i+1} = (2i+1)x - ip.$$

Therefore if it holds $\rho_{2k+1} \geq \alpha \geq (p+2)/3$ for all $k, 2k+1 \leq (p-\alpha)/2$, by the condition of Lemma 2 then $\rho_{2k+1} = (2k+1)x - kp$ for these values of k. However, if we chose $2k+1$ to be equal to the odd integer being between $(p-\alpha)/2 - 2$ and $(p-\alpha)/2$ then $k \geq (p-\alpha-5)/4$ and

$$\rho_{2k+1} = x - k(p-2x) \leq x - \frac{p-\alpha-5}{4}(p-2x) = x\frac{p-\alpha-3}{2} - p\frac{p-\alpha-5}{4}$$
$$\leq \frac{p-3}{2}\frac{p-\alpha-3}{2} - p\frac{p-\alpha-5}{4} = \frac{3\alpha-p+9}{4}.$$

Since $(p+2)/3 \leq \alpha \leq (p-3)/2$ and $p \geq 13$, the last expression is less or equal $(\alpha+6)/4 < \alpha$.

2. Let $x \geq (p+1)/2$. We shall prove by induction that if $\rho_1, \ldots, \rho_{k-1} \geq (p+2)/3$ then $\rho_k = kx - (k-1)p$.

It is true for $k \leq 2 : \rho_1 = x$ and $\rho_2 = 2x - p$ because $2x > p$. So we may assume that $k \geq 3$.

Let $\rho_{k-1} = (k-1)x - (k-2)p \geq (p+2)/3$. Then it follows $kx < kp$ from $x \leq p-3$. On the other hand

$$kx = \frac{k}{k-1}(\rho_{k-1} + (k-2)p)$$
$$\geq \frac{k}{k-1}\left(\frac{p+2}{3} + (k-2)p\right) = (k-1)p + \frac{(k-3)p + 2k}{3(k-1)}.$$

The last summand is greater than $(k-1)p$ because $k \geq 3$. Hence $\rho_k = kx - (k-1)p$. Then we have for $k = [(p-\alpha)/3] + 1$:

$$\rho_k = p - k(p-x) < p - 3\frac{p-\alpha}{3} = \alpha.$$

3. Let $x = (p-1)/2$ and $k = 2[(p-\alpha+2)/4] - 1$. Then

$$kx = \left(\frac{p-\alpha+2}{4} - \frac{1}{2}\right)(p-1) \equiv \frac{p+1}{2} - \frac{p-\alpha+2}{4} (\mathrm{mod}\ p).$$

It is evidently that the right side of this congruence is equal to ρ_k. If $\rho_k \geq \alpha$ we obtain:

$$\alpha < \frac{p+1}{2} - \frac{p-\alpha+2}{4} + 1,$$

i.e. $\alpha < (p+4)/3$. Since α is an integer and $\alpha \geq (p+2)/3$, the assertion of Lemma is proved. □

Now we are able to describe the 3-generated modifications.

Theorem 2. *If $r = 3$ then under suitable choice of a generator of G*

$$T = \langle b_1, b_m, b_{p-1} | b_1^m = b_m^2 = b_{p-1}^{p-m} = 0 \rangle,$$

where $2 \leq m \leq p-2$.

Proof. Let

$$T = \langle b_k, b_m, b_n | b_k^\alpha = b_m^\beta = b_n^\gamma = 0 \rangle,$$

where

$$\alpha + \beta + \gamma = p + 2 \tag{1}$$

and $2 \leq \alpha, \beta, \gamma \leq p-2$ (whence $p \geq 5$). It is possible to choose the generator of G such that $k = 1$. Furthermore, we may assume that $\alpha \geq \beta, \gamma$ and $m < n$.

At first we shall show that $n = p-1$. Let $n < p-1$ on the contrary. Then it follows from (1) that $\alpha \geq (p+2)/3$ and either $\beta - 1$ or $\gamma - 1$ is $\geq (p-\alpha)/2$.

Let $\beta - 1 \geq (p - \alpha)/2$ for example. Since $b_k = b_1^k \notin \langle b_m \rangle$ for $k < \alpha$ all residues of $m, 2m, (\beta - 1)m$ are $\geq \alpha$ and we have from Lemma 2 $\alpha = (p + 2)/3, m = (p - 1)/2$. But then $\beta \geq (p + 2)/3$ and $\alpha \geq \beta$ implies $\alpha = \beta = \gamma$. Again using Lemma 2 and taking into account that $n > m$ we obtain $n = p - 2$.

If $b_m^4 \neq 0$ then $b_m^4 = b_{p-2} = b_n$ what is impossible. So $\beta \leq 4$ whence $p = 7$ and

$$T = \langle b_1, b_3, b_5 | b_1^3 = b_3^3 = b_5^3 = 0 \rangle .$$

However one can check easily that such a modification doesn't exist.

The case $\gamma - 1 \geq (p - \alpha)/2$ is considered analogously.

Therefore $n = p - 1$ and

$$\begin{aligned} \langle b_{p-1} \rangle &= \{b_{p-\gamma+1}, b_{p-\gamma+2}, \ldots, b_{p-1}\} \cup 0 \\ \langle b_m \rangle &= \{b_\alpha, b_{\alpha+1}, \ldots, b_{p-\gamma}\} \cup 0. \end{aligned} \tag{2}$$

Lemma 3. *If* (2) *carries out then the inequalities*

$$km \geq (k-1)p$$

$$\frac{\alpha + (k-1)p}{k} \leq m \leq p - \gamma$$

are true for all $k \leq \beta - 1$.

Proof of Lemma. For $k = 1$ first inequality is evident and last one turns to the form

$$\alpha \leq m \leq p - \gamma$$

what follows from (2).

Let Lemma was proved for $k - 1$, i.e.

$$(k-1)m \geq (k-2)p \tag{3}$$

$$\frac{\alpha + (k-2)p}{k-1} \leq m \leq p - \gamma. \tag{4}$$

Suppose that $km < (k-1)p, k \geq 2$. Since $km > (k-2)p$ from (3) then

$$b_m^k = b_{km-(k-2)p}$$

whence

$$\alpha \le km - (k-2)p \le p - \gamma, \quad \frac{\alpha + (k-2)p}{k} \le m \le \frac{(k-1)p - \gamma}{k}.$$

From here and (4) it follows

$$\frac{\alpha + (k-2)p}{k-1} \le \frac{(k-1)p - \gamma}{k}, \quad \text{i.e.} \quad k\alpha + (k-1)\gamma \le p.$$

In particular, for $k = 2$ we have:

$$2\alpha + \gamma \le p = \alpha + \beta + \gamma - 2, \qquad \beta \ge \alpha + 2,$$

in contradiction with maximality of α.

Hence $km \ge (k-1)p$. But then it follows from $b_m^k = b_{km-(k-1)p}$ that

$$\alpha \le km - (k-1)p \le p - \gamma$$

whence

$$m \ge \frac{\alpha + (k-1)p}{k}. \qquad \square$$

Ending of the proof of Theorem 2. For $k = \beta - 1$ we obtain consecutively:

$$\frac{\alpha + (\beta-2)p}{\beta - 1} \le p - \gamma, \quad \beta\gamma - \beta \le 2\gamma - 2, \quad \beta \le 2.$$

Therefore $\beta = 2, \langle b_m \rangle = \{b_m, 0\}$ and $\alpha = p - \gamma = m$. $\square$

Finally we formulate two problems:

1. Find necessary and sufficient conditions under which the nilpotent semigroup with 0-cancellation is a modification of some finite group.

2. Let $\mathfrak{M}$ be the set of all modifications of a given group G, which are different from G^0(G with a joined zero). Let us define a partial order on $\mathfrak{M}$: $G(*) > G(\circ) \Leftrightarrow \forall x, y \in G(x * y = 0 \Rightarrow x \circ y = 0)$. Describe the maximal elements of poset $\mathfrak{M}$ (at least for $G = \mathbb{Z}_p$).

References

[1] R. Doss, *Sur l'immersion d'une demi-groupe dans un groupe*, Bull.Sci. Math. **72** (1948), 139–150.

[2] B.V. Novikov, *On partial cohomologies of semigroups*, Semigroup Forum **28** (1984), 353–364.

[3] B.V. Novikov, *On the Brauer monoid*, Matem. Zametki (in Russian, submitted).

[4] M.E. Sweedler, *Weak cohomology*, Contemp. Math. **13** (1982), 109–119.

Saltovskoye shosse 258, apt. 20, 310178 Kharkov, Ukraine