Rendiconti di Matematica, Serie VII
Volume 15, Roma (1995), 161-172

A classification of abelian quasigroups

J. SCHWENK

RIASSUNTO: *È nota la classificazione dei quasigruppi abeliani a meno di isotopie ([2], [9]). In questo lavoro si generalizza questa classificazione a meno di isomorfismi. Allo scopo vengono usati i sistemi estesi di terne corrispondenti.*

ABSTRACT:*We extend the classification of abelian quasigroups from isotopy classes, which was done in [2] and [9], to isomorphy classes. For this purpose we use the concept of an extended triple system in order to state our results.*

1 – Introduction

A well-known fact from algebraic geometry is that elliptic curves in a projective plane form an abelian group. ETHERINGTON [5] observed that certain proofs can be simplified if one uses the quasigroup structure of cubic curves. Here the product $a \circ b$ ($a \circ a$, resp.) is defined to be the third intersection point of the line through a and b (the tangent to C at a, resp.) with the cubic C (counting multiplicities). The quasigroups which are defined this way turn out to be *totally symmetric* (i. e. each equation $a \circ b = c$ implies the other five equations obtained by permuting

KEY WORDS AND PHRASES: *Abelian quasigroups – Totally symmetric quasigroups – Entropic law – Extended triple systems – Elliptic curves*
A.M.S. CLASSIFICATION: 05B07 – 20N05
This work was done while the author received a research grant from the University of Gießen.

a, b and c) and *entropic* (i. e. $(a \circ b) \circ (c \circ d) = (a \circ c) \circ (b \circ d)$ holds for all elements a, b, c, d of the quasigroup).

MURDOCH and BRUCK ([9], [2]) showed that each entropic totally symmetric quasigroup is isotopic to exactly one abelian group, and that all such quasigroups can be constructed from abelian groups. Therefore we call them *abelian quasigroups*.

Extended triple systems have been defined and studied in a number of papers by BENNET, MENDELSOHN and JOHNSON ([1], [8]). They are the geometric analogues of totally symmetric quasigroups. It will be useful to formulate our results in terms of extended triple systems rather than quasigroups, because we will use geometric expressions like "tree" and "circle" to state our results. An extended triple systems is called *abelian* if the corresponding quasigroup is abelian.

An excellent introduction to the interaction between combinatorial and algebraic structures is the section on the construction of big Steiner triple systems from smaller ones via the direct product of quasigroups given by BRUCK in [4].

Abelian extended triple systems that are embedded in a projective plane have already been studied in order to generalize SEGRE's theorem [11] from quadratic to cubic curves. They have been called *graphic curves* [12], *abelian arcs* [6], *graphic arcs* [10] and *cubic arcs* [7], and embeddings of these structures into cubic curves have been proved under certain conditions. In this article, we look at abelian arcs *not* embedded in a projective plane.

Our main results are the following: Let G be an finite abelian group.

- If 3 does not divide $|G|$, then there is up to isomorphism exactly one abelian extended triple system that is isotopic to G.
- If in the unique decomposition of G into cyclic subgroups of prime power order there are exactly k nonisomorphic cyclic factors of order 3^x, then there are exactly $k+1$ nonisomorphic abelian extended triple systems that are isotopic to G.

2 – Basic Definitions

2.1 – Quasigroups

DEFINITION. (a) *A* quasigroup *is a set Q together with a binary*

operation $\cdot$ where the equations $ax = b$ and $ya = b$ have unique solutions in Q for all $a, b \in Q$.

(b) *A quasigroup Q is called* abelian *if it satisfies the equations $ab = ba$, $a(ab) = b$ and $(ab)(cd) = (ac)(bd)$ for all $a, b, c, d \in Q$. Here the first two equations guarantee that the quasigroup is totally symmetric, and the third one is the entropic law.*

(c) *Two quasigroups $(Q, \cdot)$ and $(R, \circ)$ are* isotopic *if there is a triple (α, β, γ) of bijective maps from Q to R such that*

$$a^\alpha \circ b^\beta = (a \cdot b)^\gamma \quad \forall a, b \in Q.$$

In case that $\gamma = id$, R is called a principal isotope *of Q.*

The concept of isotopy looks quite complicated. However it becomes clear if we look at the Caley table of a quasigroup. Isotopic quasigroups have Caley tables that differ only in the choice of the set Q and a row and a column permutation. Isotopy and principal isotopy are equivalence relations on the set of all quasigroups.

Definition. (a) *Let $(G, +)$ be an abelian group, and let e be a fixed element of G. Then we can define a quasigroup $(Q(G, e), \cdot)$ by*

$$a \cdot b := e - a - b.$$

(b) *Let $(Q, \cdot)$ be an abelian quasigroup, and let o be a fixed element of Q. We define $(G(Q, o), +)$ by*

$$a + b = (ab)o.$$

The group G is isotopic to the quasigroup $Q(G, e)$, and the same holds for Q and $G(Q, o)$. The quasigroup $Q(G, e)$ is abelian, and $G(Q, o)$ is an abelian group.

The next lemma, which we give without proof, shows that each abelian quasigroup can be constructed this way.

Lemma 2.1. *Let Q be an abelian quasigroup, and let $G = G(Q, o)$. Then $Q = Q(G, o^2)$.*

The following theorem of BRUCK states that the group isotopic to an abelian quasigroup is unique, using the fact that isotopy is an equivalence relation.

THEOREM 2.2 ([3]). *If two groups are isotopic, then they are isomorphic as well.*

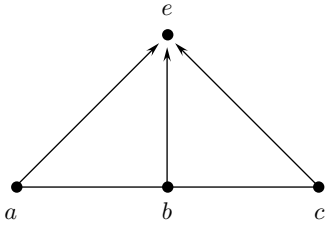
We now know that there is a bijective correspondance between the isomorphy classes of abelian groups and the isotopy classes of abelian quasigroups. We will now investigate the number of isomorphy classes of abelian quasigroups inside each isotopy class.

2.2 – Extended Triple Systems

Extended triple systems were introduced by BENNET, MENDELSOHN and JOHNSON ([8], [1]) as a generalization of Steiner triple systems. In Steiner triple systems, through any two different points there is exactly one triple. We obtain extended triple systems if we allow the two points to be equal.

DEFINITION. *An* extended triple system *(ETS) is a pair (E, T) where E is a set (of points) and T is a collection of unordered triples of elements of E such that any two (not necessarily different) points lie in exactly one triple of T.*

EXAMPLE (1) Let $E = \{a, b, c, e\}$ and $T = \{[a, b, c],\ [a, a, e],\ [b, b, e],\ [c, c, e],\ [e, e, e]\}$. Then (E, T) is an extended triple system.



(2) From a Steiner triple system S we obtain two different extended triple systems: the first one by adding the triples $[a, a, a]$ for all $a \in S$, and the second one by adding a point e and the triples $[e, e, e], [a, a, e]$ for all $a \in S$. These constructions are due to BRUCK [4].

(3) The points of an elliptic curve C in a projective plane P are the points of an extended triple system, and the triples are given by the lines of P meeting C in three points (counting multiplicities).

There is a bijective correspondence between extended triple systems and totally symmetric quasigroups: The product of two points can be defined to be the third point in the triple through these two points. Conversely, any equation $ab = c$ in a totally symmetric quasigroup defines a triple $[a, b, c]$ of an extended triple system.

DEFINITION. *An extended triple system is called* abelian *if the corresponding quasigroup is abelian. If this quasigroup is $Q(G, e)$, the extended triple system will be denoted by $E(G, e)$.*

DEFINITION. *A triple of the form $[a, a, b]$ is called a* tangent *of the extended triple system* at the point *a. If $a \neq b$, such a tangent is called a* 2-line*, in contrast to the* 1-*lines $[a, a, a]$ and the* 3-*lines $[a, b, c]$ with three different points a, b and c.*

A point a is called an inflection point *if the tangent at a is a* 1-*line.*

In previous articles on extended triple systems the number of inflection points in relation to the total number of points was studied ([1], [8]).

3 – The Case "3 does not divide $|G|$"

When looking at extended triple systems as a special kind of quasigroup, only the isotopy classes have been studied. The results of ALBERT, BRUCK and MURDOCH say that in each isotopism class of an abelian quasigroup there is exactly one abelian group. These results do not tell us how many non-isomorphic abelian quasigroups there are in the isotopism class of a fixed abelian group.

We will now look at the isomorphism classes of abelian quasigroups. Our result is that in case $gcd(|G|, 3) = 1$ for each abelian group G there is up to isomorphism exactly one abelian quasigroup. The case that 3 divides the order of the group is more complicated and will be dealt with in the next section.

The following lemma is immediate.

LEMMA 3.1. $E(G,e) \times E(H,f) \cong E(G \times H,(e,f))$.

This result enables us to construct all abelian ETS from the ETS of cyclic groups. It also helps us in determining the number of isomorphy classes of abelian quasigroups isotopic to a given group. A first step in this direction is the following theorem.

THEOREM 3.2. *Let G be isomorphic to the cyclic group Z_m.*
(1) $E(G,e) \cong E(G,e+3)$.
(2) $E(G,1) \cong E(G,2)$.
(3) *If* $gcd(|G|,3) = 1$, *then* $E(G,0) \cong E(G,1)$.

PROOF. Use the maps $\alpha : a \mapsto a+1$, $\beta : a \mapsto -a+1$ and $\gamma_1 : a \mapsto a+k$ $\gamma_2 : a \mapsto a+(2k-1)$, resp. □

4 – The Case "3 divides $|G|$"

We will distinguish nonisomorphic abelian extended triple systems by the structure of the set of their 2-lines.

DEFINITION. *The graph formed by the points of an extended triple system E together with all 2-lines of E is called the* 2-shape *of E.*

In the following we shall use graph-theoretic language, for instance we shall speak of circles.

In a tangent $[a,a,b]$ of $E(G,e)$ the element b is given by the equation

$$a \circ a = e - 2a.$$

Therefore the number -2 will play an important role in our proofs, and we need the following lemma.

LEMMA 4.1. *The order $ord(3^r,-2)$ of -2 in the group $(Z_{3^r}^*,\cdot)$ is*

$$ord(3^r,-2) = 3^{r-1}.$$

PROOF. First we prove by induction on r that there is an integer x not divisible by 3 such that

$$1-(-2)^{3^{r-1}}=3^r x \quad (*).$$

For $r=0$ we get $1-(-2)^{3^0}=3$.

Now we assume that there is a positive integer y relatively prime to 3 such that $1-(-2)^{3^{t-1}}=3^t y$. We get

$$\begin{aligned}1-(-2)^{3^t} &= 1-((-2)^{3^{t-1}})^3 = 1-(1-3^t y)^3 = \\ &= 1-(1-3(3^t y)+3(3^t y)^2-(3^t y)^3) = \\ &= 3^{t+1}(y-3^t y^2+3^{2t-1}y^3) = 3^{t+1}x\end{aligned}$$

and x is not divisible by 3 since $x \equiv y \pmod 3$.

The order of -2 has to be a divisor of the group order $3^{r-1}2$; more precisely, because of $(*)$ it has to divide 3^{r-1}. Since equation $(*)$ holds for all integers r it follows that $1-(-2)^{3^{s-1}} \not\equiv 0 \pmod{3^r}$ for $s<r$. This proves that the multiplicative order of -2 modulo 3^r is 3^{r-1}. □

Since $E(G\times H,(e,f))=E(G,e)\times E(H,f)$, we can solve the problem by first looking at cyclic groups $(Z_{3^r},+)$ and their extended triple systems $E(Z_{3^r},0)$ and $E(Z_{3^r},1)$, and then considering direct products.

THEOREM 4.2. *In the 2-shape of $E(Z_{3^r},0)$, each element which has the form $y=3^s x, \quad gcd(x,3)=1$, lies on a circle of lenght 3^{r-s-1}.*

PROOF. Consider the sequence

$$y_0=y, y_{n+1}=y_n\circ y_n=(-2)^{n+1}y \quad (n\in N).$$

Then $y_m=(-2)^m y=y_0=y \pmod{3^r}$ is equivalent to $(-2)^m=1 \pmod{3^{r-s}}$ since then

$$(-2)^m y=(3^{r-s}z+1)3^s x=3^r zx+3^s x=3^s x=y \pmod{3^r}.$$

So the lenght m of the circle is equal to $ord(3^{r-s},-2)$, which is 3^{r-s-1} by the previous lemma. □

THEOREM 4.3. *The 2-shape of $E(Z_{3^r}, 1)$ consists of a single circle of lenght 3^r.*

PROOF. By induction we show that in $Q(Z_m, e)$ we have

$$(\overbrace{(a^2)^2 \cdots)^2}^{n} =: a^{2^n} = e \cdot \sum_{k=0}^{n-1} (-2)^k + a(-2)^n \pmod{m}.$$

We can get rid of the sum in the above expression by using the equation

$$3 \sum_{k=0}^{n-1} (-2)^k = 1 - (-2)^n .$$

Finally, we get for $E(Z_{3^r}, 1)$:

$$\begin{aligned} a^{2^n} = a \pmod{3^r} &\iff (1 - (-2)^n) = 3a(1 - (-2)^n) \pmod{3^{r+1}} \\ &\iff 0 = (3a - 1)(1 - (-2)^n) \pmod{3^{r+1}}. \end{aligned}$$

Since $3a - 1$ is always relatively prime to 3, the equation reduces to $0 = 1 - (-2)^n \pmod{3^{r+1}}$ and now lemma 4.1 proves the theorem. □

The next step in our argument is to prove a lemma which tells us what happens with circles when we take direct products.

LEMMA 4.4. *Let E and F be extended triple systems, and let the points $e \in E$ and $f \in F$ lie on circles of length m and n, respectively. Then (e, f) lies on a circle of length* $\operatorname{lcm}(m, n)$.

PROOF. If $e^{2^m} = e$ and $f^{2^n} = f$, then the smallest integer k with $(e^{2^k}, f^{2^k}) = (e, f)$ is $k := lcm(m, n)$. □

We now have the following list: Let G be a cyclic group of order 3^r, and let H be a cyclic group of order 3^s with $r \leq s$.

Extended triple system	2-shape
$E(G,0)$	circles of length $1,3,\ldots,3^{r-1}$
$E(G,1)$	circle of length 3^r
$E(H,0)$	circles of length $1,3,\ldots,3^{s-1}$
$E(H,1)$	circle of length 3^s
$E(G\times H,(0,0))$	circles of length $1,3,\ldots,3^{s-1}$
$E(G\times H,(0,1))$	circle of length 3^s
$E(G\times H,(1,0))$	circles of length $3^r,\ldots,3^{s-1}$
$E(G\times H,(1,1))$	circle of length 3^s

LEMMA 4.5. *For $G\cong Z_{3^r}$ and $H\cong Z_{3^s}$ with $r\le s$ we have*

$$E(G\times H,(0,1))\cong E(G\times H,(1,1)).$$

PROOF. In this proof, we use the notation x MOD n to denote the number $0\le y<n$ with $y\equiv x \pmod n$.

The map $\alpha : E(G\times H,(0,1))\to E(G\times H,(1,1))$ defined by

$$\alpha(a,b) := ((a+b) \text{ MOD } 3^r, b).$$

is bijective, because we have the inverse map

$$\alpha^{-1}(a,b) := ((a-b) \text{ MOD } 3^r, b).$$

It sends lines to lines: from $a_1+a_2+a_3\equiv 0 \pmod{3^r}$ and $b_1+b_2+b_3\equiv 1 \pmod{3^s}$ it follows that

$$\sum_{i=1}^{3}((a_i+b_i) \text{ MOD } 3^r)\equiv\sum_{i=1}^{3}a_i+\sum_{i=1}^{3}(b_i \text{ MOD } 3^r)\equiv 0+1=1 \pmod{3^r}.$$

So α is the isomorphism we were looking for. □

We can now summarize our result as follows:

THEOREM 4.6. *Let G be an abelian group of order $3^n m$, $gcd(m,3) = 1$. Let the subgroup H of order 3^n be isomorphic to*

$$\underbrace{Z_{3^{r_1}} \times \ldots \times Z_{3^{r_1}}}_{l_1} \times \ldots \times \underbrace{Z_{3^{r_k}} \times \ldots \times Z_{3^{r_k}}}_{l_k}$$

with $l_1 r_1 + \ldots + l_k r_k = n, r_1 < \ldots < r_k$. Then there are exactly $k+1$ nonisomorphic abelian extended triple systems isotopic to G.

PROOF. By repeatedly applying lemma 4.5 we see that if we have a 1 for a cyclic component $Z_{3^{r_j}}$, then it does not matter if we chose a 0 or a 1 for any component $Z_{3^{r_i}}$ with $r_i \leq r_j$. So we get all isomorphy classes if we choose a number $j \in \{0, 1, \ldots, k\}$ and then choose a 1 for the cyclic component $Z_{3^{r_j}}$ (0 means that we choose only zeros). □

5 – Finitely generated abelian groups

If we have direct products of the infinite cyclic group Z, the situation is very similar to the previous case.

THEOREM 5.1. (1) $E(Z,e) \cong E(Z,e+3)$
(2) $E(Z,1) \cong E(Z,2)$.

PROOF. We can use the same maps as for the proof of theorem 3.2. □

LEMMA 5.2. $E(Z,0) \ncong E(Z,1)$.

PROOF. The element 0 is an inflection point of $E(Z,0)$, whereas in $E(Z,1)$ there are no inflection points. □

LEMMA 5.3. $E(Z \times Z, (0,1)) \cong E(Z \times Z, (1,1))$.

PROOF. The map $\alpha : (a,b) \mapsto (a+b,b)$ is bijective and maps lines onto lines. □

LEMMA 5.4. $E(Z_{3^r} \times Z, (0,1)) \cong E(Z_{3^r} \times Z, (1,1))$.

PROOF. Use the map $\beta : (a,b) \mapsto (a + b \,\mathrm{MOD}\, 3^r, b)$. □

We get the following theorem.

THEOREM 5.5. *Let G be a finitely generated abelian group. If k is the number of nonisomorphic direct factors of G of the form Z_{3^x}, $x \in N$, and $|G| > \infty$, then there are exactly $k+2$ nonisomorphic abelian extended triple systems isotopic to G.*

PROOF. We can write G as $G \cong H \times \mathbf{Z}^t$ where H is a finite abelian group. Let the corresponding extended triple systems be denoted by $E(H \times \mathbf{Z}^t, (a, z_1, \ldots, z_t))$. If we choose all the z_i $(i = 1, \ldots, t)$ to be 0, then the difference in the structure comes from the finite part $E(H, a)$, since a complete copy of this extended triple system is fixed to the inflection point of $E(\mathbf{Z}^t, (0, \ldots, 0))$. In this case there are $k+1$ different extended triple systems according to theorem 4.6. If some z_i is chosen to be 1, the whole structure is dominated by $E(\mathbf{Z}, 1)$ as shown in the two previous lemmata. This adds one further non-isomorphic extended triple system, so the total number is $k+2$. □

6 – Open problems

An interesting open problem is whether all abelian extended triple systems embeddable in a projective plane $PG(2,q)$ can be characterized as the point set of a cubic curve. In this case it would follow (apart from some special cases) that only those abelian extended triple systems can be embedded where the corresponding group is a direct product of at most two cyclic factors. We were able to prove one result in this direction, namely that any extended triple system $E(G,0)$, where G contains a subgroup isomorphic to $Z_{2p} \times Z_2 \times Z_2$, $p \neq 3$ a prime, is not embeddable in a desarguesian projective plane.

REFERENCES

[1] F.E. Bennett – N. S. Mendelsohn: *On the Existence of Extended Triple Systems*, Utilitas Mathematica 14 (1978), 249-267.

[2] R.H. Bruck: *Some results in the theory of quasigroups*, Trans. Am. Math. Soc. **55** (1944), 19-52.

[3] R.H. Bruck: *A survey of binary systems*, Springer-Verlag, 1958.

[4] R.H. Bruck: *What is a loop?*, In: Studies in modern algebra (A. A. Albert, ed.), Prentice-Hall, Englewood-Cliffs, N.J., 1963, 59-99.

[5] I.M.H. Etherington: *Quasigroups and cubic curves*, Proc. Ed. Math. Soc., (2), **14** (1964/65), 273-291.

[6] D. Ghinelli – N. Melone –U. Ott: *On abelian cubic arcs.*, Geom. Dedicata, **32** (1989), 31-52.

[7] J.W.P. Hirschfeld – J.F. Voloch: *The characterization of elliptic curves over finite fields*, J. Austr. Math. Soc., **45** (A) (1988), 275-286.

[8] D.M. Johnson – N.S. Mendelsohn: *Extended Triple Systems*, Aequationes Math., **3** (1972), 291-298.

[9] D.C. Murdoch: *Structure of abelian quasigroups*, Trans. Am. Math. Soc., **49** (1941), 392-409.

[10] G. Raguso – L. Rella: *On the graphic arcs embeddable in an algebraic plane curve*, Mitt. Math. Sem. Gießen, **169** (1985), 45-53.

[11] B. Segre: *Ovals in a finite projective plane*, Canad. J. Math., **7** (1955), 414-416.

[12] M. Tallini-Scafati: *Graphic curves on a Galois plane*, In: Atti Conv. Geom. e sue Appl. Perugia, 395-401, 1970.

Lavoro pervenuto alla redazione il 1 settembre 1993
modificato il 5 dicembre 1994
ed accettato per la pubblicazione il 26 dicembre 1994.
Bozze licenziate il 30 gennaio 1995

Indirizzo dell'Autore:

Jörg Schwenk – Deutsche Telekom – Forschungs- und Technologiezentrum – Am Kavalleriesand 3 – 64295 Darmstadt