An Introduction to Commutative Trinary Groups

Kyle Miller

23 July 2010

Abstract

In this document, we will define the notion of a commutative trinary group, which is group-like algebraic object with an associated trinary operation, show basic properties of these objects, and determine the trinary subgroups of $\mathbb{F}_p^*$ useful for understanding the basic structure of quadratic residue graphs. We will only talk about trinary groups which are commutative 1) because of the difficulties inherent in non-commutative algebra and 2) because the motivation in studying trinary groups is to understand quadratic residues in $\mathbb{F}_p^*$.

1 Introduction

A commutative trinary group is a nonempty set G and an operation $f : G \times G \times G \to G$ which satisfies the following axioms:

1. *Commutativity.* For all $a, b, c \in G$, $f(a, b, c) = f(a, c, b) = f(b, a, c) = f(b, c, a) = f(c, a, b) = f(c, b, a)$.
2. *Associativity.* For all $a, b, c, d, e \in G$, $f(f(a, b, c), d, e) = f(a, f(b, c, d), e) = f(a, b, f(c, d, e))$.
3. *Inverses.* For all $b \in G$, there exists an $x \in G$ such that $f(a, b, x) = a$ for all $a \in G$.

We will tend to use infix or juxtaposition notation such as $f(a, b, c) = abc$ or $f(a, b, c) = a+b+c$, which is unambiguous due to the property of associativity. We will also assume that G is finite unless otherwise specified.

First, we will give some very straightforward properties to aid in checking the axioms.

- Since a transposition and a 3-rotation together generate S_3, for the commutativity property, we need only check $abc = bac = bca$ for all $a, b, c \in G$.
- It then follows that we only need to check $(abc)de = a(bcd)e$ once we determine commutativity to show associativity.

If we are given an abelian group G, we can induce a trinary group operation f defined by $f(a, b, c) = abc$ where multiplication is done using the binary operation. That commutativity and associativity are inherited is clear. We see that inverses are also induced: say $b \in G$ and b^{-1} is the inverse of b under the binary group operation. Then, for any $a \in G$, $f(a, b, b^{-1}) = abb^{-1} = a$.

Note that there is no property of identity in a commutative trinary group. Without first definining one, let's call $i \in G$ an identity element. The property $ai = a$ is meaningless in G because there is no binary operation. Because of this, one may instead try $abi = ab$, but again, there is no binary operation. This leads to the following definition:

Definition 1. *An element $i \in G$ is called an identity of G if, for all $a \in G$, $aii = a$.*

If there is an identity element $i \in G$, we may induce a binary operation $g : G \times G \to G$ defined by $a, b \mapsto abi$ to turn G into a binary commutative group. We will verify this. Assume $a, b, c \in G$:

- *Closure.* $g(a, b) = abi \in G$ since G is a trinary group.
- *Identity.* $g(a, i) = aii = a$.
- *Associativity.* $g(g(a, b), c) = (abi)ci = a(bci)i = g(a, g(b, c))$.
- *Inverses.* Let $x \in G$ be such that $iax = i$. Then $g(a, x) = axi = i$, so $x = a^{-1}$.

However, such inverse elements are not necessarily unique, so many groups may be induced. For instance, if $G = \mathbb{Z}/8\mathbb{Z}$, both 0 and 4 are identity elements since $a+0+0 = a$ and $a+4+4 = a$. This gives us two binary group operations $g_1(x, y) = x + y$ and $g_2(x, y) = x + y + 4$. These groups, however, are isomorphic, with $\varphi : G_1 \to G_2$ defined by $\varphi(x) = x + 4$.

We see that if i is an identity element that $iii = i$. It is indeed the case that the implication may be reversed, and this will be shown shortly.

Now, we will look at some basic properties for manipulating elements in these groups.

- Say $b, c \in G$. Then there exist $x, y \in G$ so that $(abc)xy = a$ for all $a \in G$. This follows from two applications of the inverse existence axiom: first, there exists an $x \in G$ so that $(aby)cx = aby$, and second, there exists a $y \in G$ so that $aby = a$. Thus, $(abc)xy = a$.
- *Cancellation law.* If $abx_1 = abx_2$ for $a, b, x_1, x_2 \in G$, then $x_1 = x_2$. This follows from the previous property: there exist $\alpha, \beta \in G$ so that $x_i ab\alpha\beta = x_i$ for every value x_i, which implies $x_1 = abx_1\alpha\beta = abx_2\alpha\beta = x_2$.
- Inverses are unique. Say $b \in G$ and $x_1, x_2 \in G$ are such that $abx_i = a$ for all $a \in G$. Then $abx_1 = abx_2$, and $x_1 = x_2$ follows from the cancellation law.
- Say $i \in G$. Then $iii = i \implies i$ is an identity of G. We see for $b \in G$, $bii = b(iii)i = (bii)ii$. By the cancellation law, $bii = i$.

2 Trinary Subgroups

A trinary subgroup of a commutative trinary group G is a nonempty subset $H \subset G$ which is closed under the operation of G and which has the axiom of inverses.

A coset of a trinary subgroup H, analogous to a coset of a binary subgroup, is a set $abH = \{abh \mid h \in H\}$ for $a, b \in G$. We will also use the same notation $abS = \{abs \mid s \in S\}$ for any subset $S \subset G$.

For any $a, b \in G$, we can see there exist $\alpha, \beta \in G$ so that $\alpha\beta(abH) = H$. Say $x \in abH$. Then $x = abh$ for some $h \in H$, so there exist $\alpha, \beta \in G$ so that $\alpha\beta x = h$. Thus, $\alpha\beta(abH) \subset H$. Now, say $h \in H$. Then, using the same α and β for the given a and b, we see $h = \alpha\beta(abh)$, which implies $H \subset \alpha\beta(abH)$.

A corollary to this is that $|H| = |abH|$ for every $a, b \in G$.

Theorem 2. *Either $(abH) \cap (a'b'H) = \varnothing$ or $abH = a'b'H$ for any $a, b, a', b' \in G$.*

Proof. Assume the intersection is non-empty, that there is an $x \in (abH) \cap (a'b'H)$. Then $x = abh = a'b'h'$ for some $h, h' \in H$. Let $y \in abH$, so $y = ab\eta$ for some $\eta \in H$. There exist $h^{-1}, b^{-1} \in G$ so $xh^{-1}b^{-1} = a$, which implies $y = (xh^{-1}b^{-1})b\eta = xh^{-1}\eta = (a'h'b')h^{-1}\eta = a'b'(h'h^{-1}\eta)$. Since $h', h^{-1}, \eta \in H$ and H is closed under the trinary operation, $h'h^{-1}\eta \in H$, so $y \in a'b'H$, and thus $abH \subset a'b'H$. Similarly, we can go the other way to show $abH \supset a'b'H$, and therefore $abH = a'b'H$ if the intersection is non-empty.

Now assume the intersection is empty. Then it's clear that $abH \neq a'b'H$. $\square$

Corollary 3. *The cosets of H partition G.*

It follows that $|H|\,k = |G|$ for some integer k. We call this k the index of H in G, or $[G : H]$.

Corollary 4 (Counting Theorem)**.** *Let H be a trinary subgroup of G. Then $|G| = [G : H]\,|H|$.*

We can generate a trinary subgroup from an element $x \in G$ by taking all powers of x^k with $k = 2i + 1$ for all integers i. We represent this trinary subgroup by $\langle x \rangle$. Also, by the counting theorem, $|\langle x \rangle|$ divides $|G|$ for all x. For instance, with $1 \in \mathbb{Z}/8\mathbb{Z}$, $\langle 1 \rangle = \{1, 3, 5, 7\}$, and $4 \mid 8$.

3 Homomorphisms

A homomorphism $\varphi : G \to G'$ between two commutative trinary groups G and G' satisfies $\varphi(abc) = \varphi(a)\varphi(b)\varphi(c)$, for all $a, b, c \in G$.

The image of φ is a trinary group:

- *Closure.* For $\alpha, \beta, \gamma \in \varphi(G)$, there exist $a, b, c \in G$ such that $\varphi(a) = \alpha$, $\varphi(b) = \beta$, and $\varphi(c) = \gamma$. Thus, $\alpha\beta\gamma = \varphi(a)\varphi(b)\varphi(c) = \varphi(abc) \in \varphi(G)$.

- *Inverses.* Say $\beta \in \varphi(G)$. Let $\alpha \in \varphi(G)$, and let $a, b \in G$ be such that $\varphi(a) = \alpha$ and $\varphi(b) = \beta$. Then there exists an $x \in G$ such that $abx = a$, which implies $\varphi(abx) = \varphi(a)$, so $\alpha\beta\varphi(x) = \alpha$.

Then, by the counting theorem, $|\varphi(G)|$ divides $|G'|$.

Theorem 5. *All $\varphi^{-1}(x)$ are of the same cardinality, where $x \in \varphi(G)$.*

Proof. We will show $\left|\varphi^{-1}(x_1)\right| = \left|\varphi^{-1}(x_2)\right|$ for all $x_1, x_2 \in \varphi(G)$. To do this, we will first show that each element of $\varphi^{-1}(x_1)$ has a corresponding element in $\varphi^{-1}(x_2)$. There exists a unique $z \in \varphi(G)$ so that $ax_1z = a$ for all $a \in \varphi(G)$ since $\varphi(G)$ is a trinary subgroup. Fix some $w \in \varphi^{-1}(z)$ and some $y_2 \in \varphi^{-1}(x_2)$. Then, for all $y \in \varphi^{-1}(x_1)$, $\varphi(yy_2w) = x_1x_2z = x_2$, so $yy_2w \in \varphi^{-1}(x_2)$. Since there exist elements $\alpha, \beta \in G$ so that $\alpha\beta yy_2w = y$, the map $y \mapsto yy_2w$ is an injection, and thus $\left|\varphi^{-1}(x_1)\right| \leq \left|\varphi^{-1}(x_2)\right|$. Swapping the roles of x_1 and x_2 in the above reasoning, we conclude $\left|\varphi^{-1}(x_1)\right| = \left|\varphi^{-1}(x_2)\right|$. $\square$

This implies there is an integer k so that $|G| = k\left|\varphi^{-1}(x)\right|$ for all $x \in \varphi(G)$. And, since the fibres partition G, we arrive at the following corollary:

Corollary 6. $|G| = |\varphi(G)|\left|\varphi^{-1}(x)\right|$ *for all $x \in \varphi(G)$.*

And, as a corollary to the corollary, $|\varphi(G)|$ divides $|G|$.

If $|G| \perp |G'|$, then, since $|\varphi(G)|$ divides $|G'|$, and $|\varphi(G)|$ divides $|G|$, it must be the case that $|\varphi(G)| = 1$, so there is some $i \in G'$ so $\varphi(x) = i$ for all $x \in G$, which means $i = \varphi(xxx) = iii$, so i is an identity element of G'.

Another way we may induce a binary group from a commutative trinary group G if we have no identity element is to take a trinary subgroup $H \subset G$ and create the map $f : G \times G \to G/H$ defined by $f(x, y) = xyH$, where G/H represents the set of all cosets xyH for all $x, y \in G$. The image of f is an abelian group under the associated operation $\cdot : G/H \times G/H \to G/H$ defined by $xyH \cdot x'y'H \to xyx'y'H$:

- *Closure.* The operation generates another coset in G/H.
- *Identity.* If $x \in G$, there is an x^{-1} so $axx^{-1} = a$ for all $a \in G$. Then $H = f(x, x^{-1})$. Say $\alpha_1\alpha_2 H \in G/H$. We have $H \cdot \alpha_1\alpha_2 H = \alpha_1\alpha_2 H$.
- *Inverses.* Let $\alpha_1\alpha_2 H \in G/H$. There are $\alpha_1^{-1}, \alpha_2^{-1} \in G$ so that $a\alpha_1\alpha_2\alpha_1^{-1}\alpha_2^{-1} = a$ for all $a \in G$. Then $\alpha_1\alpha_2 H \cdot \alpha_1^{-1}\alpha_2^{-1} H = H$.

This induced group is of order $|G| / |H|$ since the cosets partition the group.

4 Trinary Subgroups of C_n

In this section we will look at some of the trinary subgroups of C_n which will be useful in the discussion of $\mathbb{F}_p$.

Let integers k, q be chosen to satisfy $n = 2^k q$ with q odd, and say $C_n = \langle x \rangle$. Then, we can create cyclic subgroups of C_n for integers $0 \le i \le k$ called $Q_i = \left\langle x^{2^{k-i}} \right\rangle$, so $|Q_i| = 2^i q$. We note that $Q_{i+1} \supset Q_i$ with $[Q_{i+1} : Q_i] = 2$ for $0 \le i < k$.

If an element $z \in C_n$ has order d, then we see that $z \in Q_i$ if $d \mid 2^i q$ since Q_i has $2^i q$ elements.

Let us define the sets $H_i = Q_i \setminus Q_{i-1}$ for $0 < i \le k$, and $H_0 = Q_0$. If $z \in H_i$, then $z \mid 2^i q$ and $z \nmid 2^{i-1} q$, which implies z is of order $2^i p$ with $p \mid q$. Therefore, H_i is the set of all elements of order $2^i p$ with $p \mid q$.

The set of cosets C_{i+1}/C_i is simply $\{C_i, H_{i+1}\} \approx C_2$. So, if we take $x_1, x_2, x_3 \in H_{i+1}$, the product $x_1x_2x_3 \in H_{i+1}$ as well. Thus, H_{i+1} is closed under trinary multiplication.

Each element $x \in H_i$ has inverse x^{-1}. Because x and x^{-1} both have the same order in the group C_n, $x^{-1} \in H_i$ as well. Therefore H_i has trinary inverses as $axx^{-1} = a$ for all $a \in H_i$.

We conclude that each H_i is a commutative trinary subgroup of C_n.

We can easily find more trinary subgroups in a similar manner by looking at the chain of subgroups $C_{2^i p}$ for $p \mid q$. For example, if $\langle x \rangle = C_n$, we have $R_i = \left\langle x^{2^i q} \right\rangle$ (so R_0 is the trivial subgroup), and thus we have $I_i = Q_i \setminus Q_{i-1}$ as commutative trinary subgroups.

5 Trinary Subgroups of $\mathbb{F}_p^*$

Since the multiplicative group $\mathbb{F}_p^*$ is cyclic and isomorphic to $\mathbb{C}_{p-1}$, we may apply the discussion above. If we take integers k, q so $p - 1 = 2^k q$ with q odd, we get the chain of cyclic subgroups Q_i as well as the trinary subgroups H_i.

If $x \in H_i$, $i > 0$, then x has order $d = 2^i p$ with $p \mid q$. We see that the order of x^2 is then $2^{i-1}p$. Therefore $x^2 \in H_{i-1}$. And, if $x \in H_0$, since $H_0 = Q_0$, $x^2 \in H_0$.

This means there are homomorphisms $\varphi : H_i \to H_{i-1}$ for all $0 < i \leq k$ and $\varphi : H_0 \to H_0$ defined by $\varphi(x) = x^2$. Note that $|H_i| = 2^{i-1}q$ for $i > 0$ and $|H_0| = q$.

Remember that if $x \in \mathbb{F}_p^*$ is a square, there are exactly two distinct elements $\alpha_1, \alpha_2 \in \mathbb{F}_p^*$ such that $x = \alpha_1^2 = \alpha_2^2$. If we look at the orders of the elements, *handwave handwave*, we also see that each φ must be surjective.

Since $\varphi : H_0 \to H_0$ is a surjection, it must be the case that φ is an automorphism, and the fibres of each element are of cardinality one. Because $|H_0| = |H_1|$, $\varphi : H_1 \to H_0$ must be an isomorphism, and the fibres are also of cardinality one. Next, for each $\varphi : H_i \to H_{i-1}$ with $i > 1$, since $|H_i| = 2\,|H_{i-1}|$ and φ is a surjection, the fibres are all of cardinality two.

If we apply this to quadratic residue graphs $(\mathbb{F}_p^*, E)$ where $\vec{xy} \in E$ if $x^2 \equiv y \pmod{p}$, we see that the graph is composed of directed rings whose elements are from H_0, and complete binary trees rooted from elements of H_1, which each then connect to the elements of H_0. And, each binary tree must be of depth k.

We previously showed each level H_i is a commutative trinary subgroup of $\mathbb{F}_p^*$.

One binary group we can induce is H_i/I_i, which has q elements. I'm fairly certain $H_i/I_i \approx C_q$. Thus, there is an element which generates H_i/I_i, and it's possible to walk around each level H_i given the 2^i-th roots of 1 (which is the set I_i).

6 Further Work

I'm not sure if there's a good geometric way for thinking about trinary groups as there is for thinking about binary groups (which is as symmetries).