Regular Commutative Semigroups

Owen Bechtel

September 24, 2023

1 Introduction

Regular commutative semigroups are a generalization of abelian groups. They are defined by replacing the "identity" and "inverse" axioms of an abelian group with the weaker requirement that every element have a "pseudoinverse." In a regular commutative semigroup (or RCS), there need not be a "global" zero element 0 such that $0 + x = x$ for all x; instead, each element x has its own "local" zero, denoted 0_x.

I came up with this generalization of an abelian group independently, and studied it for several days before learning that the axiom I was researching already had a name: regularity. According to Wikipedia, "regular semigroups are one of the most-studied classes of semigroups." However, to my knowledge, little attention has been paid to the commutative case. Nearly all of the theorems in this paper are my own; the first three (propositions 2.1, 2.2, and 2.3) are the only exceptions.

In section 2 (Regular Commutative Semigroups), I give the precise definition of an RCS, and prove several results about them. In section 3 (Classification of RCSs), I describe a universal way of constructing an RCS out of a semilattice and a diagram of abelian groups. In section 4 (Regular Semirings), I define the notion of a "regular semiring," and prove several theorems about these structures and their connection to RCSs. Finally, in section 5 (Semimodules and Semialgebras), I characterize RCSs as semimodules over the integers.

2 Regular Commutative Semigroups

Let A be a semigroup, and a, b elements of A. If $a + b + a = a$, then b is said to be a **pseudoinverse** of a. If, in addition, $b + a + b = b$, then b is said to be an **inverse** of a. (Note that, in a monoid, this is weaker than the requirement that $a + b$ equal the identity.)

A semigroup A is said to be **regular** if every element has a pseudoinverse, i.e. for all $a \in A$ there is some $b \in A$ such that $a + b + a = a$. A **regular commutative semigroup (RCS)** is a commutative semigroup which is regular.

Proposition 2.1. *Every element of a regular semigroup has at least one inverse.*

Proof. Let A be a regular semigroup, and a an element of A. By regularity, there exists $b \in A$ with $a + b + a = a$. Let $c = b + a + b$. It is easy to check that $a + c + a = a$ and $c + a + c = c$. In other words, c is an inverse of a. □

Proposition 2.2. *Every element of a commutative semigroup has at most one inverse.*

Proof. Let A be a commutative semigroup, and a an element of A. Suppose b and c are inverses of a; we have $a + b + a = a$, $b + a + b = b$, $a + c + a = a$, and $c + a + c = c$. One can show, via a chain of equalities, that b and c are equal:

$$\begin{aligned} b &= b + a + b \\ &= b + a + c + a + b \\ &= b + a + c + a + c + a + b \\ &= c + a + b + a + b + a + c \\ &= c + a + b + a + c \\ &= c + a + c \\ &= c. \end{aligned}$$

□

By combining propositions 2.1 and 2.2, we get the following:

Proposition 2.3. *Every element of an RCS has exactly one inverse.*

If x is an element of an RCS, I will denote its unique inverse as x^*, and define 0_x to be the sum $x + x^*$.

Proposition 2.4. *The following equations hold for any element x of an RCS:*

1. $0_x + x = x$
2. $0_x + x^* = x^*$
3. $0_x + 0_x = 0_x$
4. $0_{0_x} = 0_x$
5. $(0_x)^* = 0_x$
6. $(x^*)^* = x$
7. $0_{x^*} = 0_x$

Proof. The first three statements are easy: simply replace 0_x with $x + x^*$ and use the fact that x and x^* are inverses. I will prove the rest of the statements in turn.

4. $0_{0_x} = 0_x + (0_x)^* = 0_x + 0_x + (0_x)^* = 0_x$.
5. 0_x is an inverse of 0_x, since $0_x + 0_x + 0_x = 0_x$ by statement 3. Inverses are unique, so $(0_x)^* = 0_x$.
6. x is an inverse of x^*, since the "inverse" relation is symmetric. Inverses are unique, so $(x^*)^* = x$.
7. This follows from statement 6: $0_{x^*} = x^* + (x^*)^* = x^* + x = 0_x$. □

The following theorem characterizes the idempotent elements of an RCS. (An element x is called idempotent if $x + x = x$.)

Proposition 2.5. *For any element a of an RCS, the following are equivalent:*

1. *a is idempotent,*
2. *$0_a = a$,*
3. *$a = 0_x$ for some x.*

Proof. Property 2 clearly implies property 3: simply take $x = a$. Property 3 implies property 1 because $0_x + 0_x = 0_x$. All that remains is to show that property 1 implies property 2.

Suppose a is idempotent. Then a is its own inverse, because $a + a + a = a + a = a$. We then have $0_a = a + a^* = a + a = a$. □

Proposition 2.6. *The following equations hold for any elements x, y of an RCS:*

1. *$(x + y)^* = x^* + y^*$*
2. *$0_{x+y} = 0_x + 0_y$*

Proof. It is easy to check that $x^* + y^*$ is an inverse of $x + y$. Since inverses are unique, this implies $(x + y)^* = x^* + y^*$.

The second equation is a consequence of the first: we have $0_{x+y} = x + y + (x + y)^* = x + y + x^* + y^* = 0_x + 0_y$. □

I will now introduce some notation. If A is an RCS, I will define $\zeta : A \to A$ and $Z_A \subseteq A$ as follows:

- $\zeta(x) = 0_x$
- $Z_A = \{x \in A \mid x + x = x\}$

By proposition 2.6, ζ is an endomorphism of A, and by proposition 2.5, the image of ζ is Z_A. Moreover, it was shown in proposition 2.4 that $0_{0_x} = x$ for all x, which means that ζ is an idempotent function in the sense that $\zeta \circ \zeta = \zeta$. In summary, one can think of ζ as *projecting* the whole of A onto Z_A (the subset of idempotent elements) in a way that preserves addition.

For any $a \in Z_A$, I will define $G(a) \subseteq A$ to be the fiber of ζ at a. In other words, $G(a) = \{x \in A \mid 0_x = a\}$.

Proposition 2.7. *For any RCS A and for all $a \in Z_A$, $G(a)$ is an abelian group with a as its identity.*

Proof.

- $G(a)$ is closed under addition: If $0_x = 0_y = a$ then $0_{x+y} = 0_x + 0_y = a + a = a$.
- $G(a)$ has a as an identity: If $0_x = a$ then $a + x = x$.
- $G(a)$ has inverses (in the group sense): If $0_x = a$ then $0_{x^*} = a$ (since $0_{x^*} = 0_x$), and $x + x^* = a$. □

Remark. The subsets $G(a)$ are pairwise disjoint, and their union is the whole of A. (This is true for the fibers of any function.) Thus $\{G(a) \mid a \in Z_A\}$ is a partition of A into abelian groups. The following propositions describe the relationships between these groups:

Proposition 2.8. *For any RCS A and for all $a, b \in Z_A$, the function $\phi_b : A \to A$ defined by $\phi_b(x) = x + b$ is a group homomorphism from $G(a)$ to $G(a + b)$.*

Proof. First, it is necessary to show that ϕ_b maps $G(a)$ into $G(a+b)$. If $x \in G(a)$ then $0_{\phi_b(x)} = 0_{x+b} = 0_x + 0_b = a + b$. Thus $\phi_b(x) \in G(a + b)$.

All that remains is to show that ϕ_b preserves addition. We have $\phi_b(x + y) = x+y+b$ and $\phi_b(x)+\phi_b(y) = x+b+y+b = x+y+b$ (since b is idempotent). □

Proposition 2.9. *For any RCS A and for all $a, b, c \in Z_A$ such that $a+b = a+c$, the functions $\phi_b(x) = x + b$ and $\phi_c(x) = x + c$ are equal on elements of $G(a)$.*

Proof. If $x \in G(a)$, then $x = x + a$. We have $\phi_b(x) = x + b = x + a + b = x + a + c = x + c = \phi_c(x)$. □

3 Classification of RCSs

Recall that a **semilattice** is a commutative semigroup in which every element is idempotent. Every semilattice Z has a canonical partial order on its elements: if a and b are elements of Z, one says $a \leq b$ if there exists $x \in Z$ such that $a + x = b$. The set of idempotent elements of any commutative semigroup forms a semilattice.

The theorem below defines a very general way of constructing an RCS out of a semilattice and a family of abelian groups:

Theorem 3.1. *Let Z be a semilattice, and $\{G_a\}_{a\in Z}$ a Z-indexed family of abelian groups. Let $\{\phi_{a,b} : G_a \to G_b\}_{a\leq b}$ be a family of group homomorphisms indexed by pairs $a, b \in Z$ with $a \leq b$, such that $\phi_{a,a} = \mathrm{id}$ for all a, and $\phi_{b,c} \circ \phi_{a,b} = \phi_{a,c}$ for all $a \leq b \leq c$. Then the disjoint union $A = \coprod_{a\in Z} G_a$ is an RCS with $x + y$ defined as $\phi_{a,a+b}(x) + \phi_{b,a+b}(y)$ for $x \in G_a$ and $y \in G_b$.*

Remark. The required data could be defined more concisely as a semilattice Z along with a functor from $(Z, \leq)$ to the category of abelian groups.

Proof. I will check commutativity, associativity, and regularity in turn.

- Commutativity: Let $x \in G_a$ and $y \in G_b$. We have $x + y = \phi_{a,a+b}(x) + \phi_{b,a+b}(y)$, and $y + x = \phi_{b,b+a}(y) + \phi_{a,b+a}(x)$. These are equal, since addition in Z and addition in G_{a+b} are both commutative.
- Associativity: Let $x \in G_a$, $y \in G_b$, and $z \in G_c$. We have $x + (y + z) = \phi_{a,a+b+c}(x) + \phi_{b+c,a+b+c}(\phi_{b,b+c}(y) + \phi_{c,b+c}(z)) = \phi_{a,a+b+c}(x) + \phi_{b,a+b+c}(y) + \phi_{c,a+b+c}(z)$. (This uses the fact that the $\phi_{i,j}$ are homomorphisms, as well as the functorial requirement placed on them.) Evaluating $(x + y) + z$ gives the same result.
- Regularity: Let $x \in G_a$ and write $-x$ for the inverse of x in G_a. We have $x+(-x)+x = \phi_{a,a+a+a}(x)+\phi_{a,a+a+a}(-x)+\phi_{a,a+a+a}(x)$, where addition on the left side is in A and addition on the right side is in G_{a+a+a}. But $a+a+a = a$, so $\phi_{a,a+a+a}$ is the identity map, and the right side becomes $x + (-x) + x$, which is just x. □

Below are two examples of this rather useful construction.

Example 3.2. Let Z be the semilattice $\{0, \infty\}$, where $+$ and $\leq$ are as you would expect. Define G_0 to be the group $(\mathbb{Z}, +)$ of integers under addition, and G_∞ to be the trivial group whose element I will denote ∞. There is only one way to define the $\phi_{i,j}$: we have $\phi_{0,0} = \text{id}$, $\phi_{\infty,\infty} = \text{id}$, and $\phi_{0,\infty}(n) = \infty$ for all n.

The resulting RCS is the set $\mathbb{Z} \cup \infty$ where addition is defined such that $\infty + x = \infty$ for all x. The inverse of n is $-n$ for $n \in \mathbb{Z}$, and the inverse of ∞ is ∞.

Example 3.3. Let X be a topological space. Let Z be the semilattice of open subsets of X under the operation of intersection. For open sets $U, V \in Z$, we have $U \leq V$ iff $U \supseteq V$. For $U \in Z$, let G_U be the additive group of continuous functions from U to $\mathbb{R}$, and for $U, V \in Z$ such that $U \supseteq V$, let $\phi_{U,V} : G_U \to G_V$ be the homomorphism that restricts a function defined on U to one defined on V.

The resulting RCS is isomorphic to the set of pairs (U, f) where U is an open subset of X and f is a continuous function from U to $\mathbb{R}$, and where the sum $(U, f) + (V, g)$ is equal to $(U \cap V, f + g)$.

For example, if $X = \mathbb{R}$ and U is the set of positive real numbers, we would have $(U, x \mapsto \frac{1}{x}) + (\mathbb{R}, x \mapsto 2) = (U, x \mapsto \frac{1}{x} + 2)$.

Theorem 3.4. *Any RCS can be constructed by the method in theorem 3.1.*

Proof. Let A be an RCS. Let Z be the semilattice of idempotent elements of A, and for each $a \in Z$, let G_a be the set $\{x \in A \mid 0_x = a\}$. By proposition 2.7, each G_a is an abelian group. For $a, b \in Z$ such that $a \leq b$, define $\phi_{a,b} : G_a \to G_b$ as $\phi_{a,b}(x) = x + c$ where c is an element of Z such that $a + c = b$. (By proposition 2.9, this is well defined; it does not matter which c we choose.) $\phi_{a,b}$ is a group homomorphism by proposition 2.8. It is easy to check that $\phi_{a,a}$ is the identity for all $a \in Z$, and that $\phi_{b,c} \circ \phi_{a,b} = \phi_{a,c}$ for all $a \leq b \leq c$.

Applying the construction in theorem 3.1, we get an RCS whose underlying set is the same as that of A, and whose addition law is $x + y = \phi_{a,a+b}(x) + \phi_{b,a+b}(y)$, where $x \in G_a$, $y \in G_b$, and the addition on the right is in A. This simplifies to $x + b + y + a = x + a + y + b$, which is just $x + y$. □

4 Regular Semirings

For the purposes of this paper, I will define a **semiring** to be a set S equipped with two binary operations $+$ and $\cdot$ such that:

1. $(S, +)$ is a commutative semigroup.
2. $(S, \cdot)$ is a monoid.
3. $+$ and $\cdot$ together satisfy the right and left distributive laws.

Note that a semiring, under this definition, must have a multiplicative identity, but need not have an additive identity. For example, the positive integers (under the usual operations) form a semiring.

A **regular semiring** is a semiring in which the multiplicative identity has an additive pseudoinverse. In other words, a semiring S is regular iff there exists $a \in S$ such that $1 + a + 1 = 1$ (where 1 is the multiplicative identity in S).

Proposition 4.1. *If S is a regular semiring, its additive semigroup $(S, +)$ is an RCS.*

Proof. If S is regular, there exists $a \in S$ with $1 + a + 1 = 1$. Let x be an element of S. Multiplying the preceding equation by x and distributing, we find that $x + ax + x = x$. So x has a pseudoinverse. □

Proposition 4.2. *For every element x of a regular semiring, $1^*x = x1^* = x^*$ and $0_1 x = x 0_1 = 0_x$.*

Proof. 1^* denotes the inverse of 1, so $1 + 1^* + 1 = 1$ and $1^* + 1 + 1^* = 1^*$. Right-multiplying these equations by x, one finds that $x + 1^*x + x = x$ and $1^*x + x + 1^*x = 1^*x$. So 1^*x is the inverse of x, i.e. $1^*x = x^*$. Likewise, by left-multiplying the original equations by x, one finds that $x1^* = x^*$.

The second statement follows from the first: $0_1 x = (1 + 1^*)x = x + 1^*x = x + x^* = 0_x$, and likewise $x 0_1 = 0_x$. □

Proposition 4.3. *In any regular semiring S, the subsemigroup generated by $\{1, 1^*\} \subseteq S$ is in fact a subring.*

Proof. Let R be the subsemigroup generated by 1 and 1^*. For R to be a subring of S, it must be an abelian group under addition, be closed under multiplication, and contain the multiplicative identity $1 \in S$. The last of these is obviously true; I will prove the other two requirements in turn.

- Let x be an element of R. By the definition of R (and by commutativity), x can be written as a sum $1 + \cdots + 1 + 1^* + \cdots + 1^*$.

  By propositions 2.6 and 2.4, we have $0_x = 0_1 + \cdots + 0_1 + 0_{1^*} + \cdots + 0_{1^*} = 0_1 + \cdots + 0_1 = 0_1$. Thus $0_1 + x = x$ and $x + x^* = 0_1$.

  By the same propositions, we also have $x^* = 1^* + \cdots + 1^* + (1^*)^* + \cdots + (1^*)^* = 1^* + \cdots + 1^* + 1 + \cdots + 1$, and thus $x^* \in R$.

  In summary, for all $x \in R$ we have $0_1 + x = x$, $x^* \in R$, and $x + x^* = 0_1$. Thus R is an abelian group under addition, with 0_1 as its identity.

- Note that proposition 4.2 implies that $1^*1^* = (1^*)^* = 1$. Let x and y be elements of R. Each can each be written as a sum of copies of 1 and 1^*; thus the product xy can be written as a sum of copies of $1 \cdot 1$, $1 \cdot 1^*$, 1^*1, and 1^*1^*. But these are equal to 1, 1^*, 1^*, and 1 respectively, so $xy \in R$. So R is closed under multiplication. □

Proposition 4.4. *Let S and T be semirings, and $f : S \to T$ a homomorphism of semirings. If S is regular, then T is regular.*

Proof. If S is regular, there is some $a \in S$ such that $1 + a + 1 = 1$. Applying f to this equation (and using the fact that f is a homomorphism), we get $1 + f(a) + 1 = 1$. Therefore, T is also regular. □

Proposition 4.5. *Let S be a semiring. If S is regular, there is exactly one homomorphism of semirings from $\mathbb{Z}$ to S, and if S is not regular, there are no homomorphisms from $\mathbb{Z}$ to S.*

Proof. The second half follows from proposition 4.4: $\mathbb{Z}$ is a regular semiring, so if $f : \mathbb{Z} \to S$ is a homomorphism of semirings, S must be regular. If S is *not* regular, there can be no such homomorphism.

To prove the first half, let S be a regular semiring. By proposition 4.3, S contains a subring R. $\mathbb{Z}$ is initial in the category of rings, so there exists a (unique) homomorphism from $\mathbb{Z}$ to R, which can be composed with the inclusion of R into S to get a homomorphism $f : \mathbb{Z} \to S$. We have $f(1) = 1$ and $f(-1) = 1^*$ (as 1^* is the negative of $1 \in R$).

Suppose $g : \mathbb{Z} \to S$ is another homomorphism. We have $g(1) = 1$, and it is easy to show that $g(-1)$ is an inverse of $1 \in S$, so $g(-1)$ must be 1^*. The numbers 1 and -1 generate $\mathbb{Z}$, so if two homomorphisms agree on 1 and -1, they must be equal. Thus $g = f$. □

If A is a commutative semigroup, the set of endomorphisms of A forms a semiring where addition is defined pointwise and multiplication is defined by composition of endomorphisms. This semiring is called the **endomorphism semiring** of A and is denoted $\mathrm{End}(A)$. It is analogous to the endomorphism *ring* of an abelian group. The following theorem describes an important connection between RCSs and regular semirings.

Proposition 4.6. *A commutative semigroup is regular if and only if its endomorphism semiring is regular.*

Proof. Let A be an RCS. The multiplicative identity $1 \in \text{End}(A)$ (which is the identity function on A) has a pseudoinverse (in fact an inverse) $\sigma \in \text{End}(A)$ defined by $\sigma(x) = x^*$. (σ is an endomorphism by proposition 2.6.) Thus $\text{End}(A)$ is a regular semiring.

Conversely, let A be a commutative semigroup such that $\text{End}(A)$ is a regular semiring. This means there exists $\sigma \in \text{End}(A)$ such that $1 + \sigma + 1 = 1$. Let x be an element of A. We have $x + \sigma(x) + x = (1 + \sigma + 1)(x) = 1(x) = x$. Thus x has a pseudoinverse. □

5 Semimodules and Semialgebras

Recall that an **algebra** over a commutative R is a ring R' equipped with a homomorphism from R to R'. Likewise, a **module** over R is an abelian group A equipped with a ring homomorphism from R to $\text{End}(A)$.

These definitions are easily generalized to commutative semirings. I will define a **semialgebra** over a commutative semiring S to be a semiring S' equipped with a homomorphism from S to S', and define a **semimodule** over S to be a commutative semigroup A equipped with a semiring homomorphism from S to $\text{End}(A)$.

Various propositions proved in section 4 imply the following:

1. A semialgebra over $\mathbb{Z}$ is precisely a regular semiring. (Every $\mathbb{Z}$-semialgebra is a regular semiring, and every regular semiring is a $\mathbb{Z}$-semialgebra in exactly one way.) (props. 4.4 & 4.5)

2. A semimodule over $\mathbb{Z}$ is precisely an RCS. (Every $\mathbb{Z}$-semimodule is an RCS, and every RCS is a $\mathbb{Z}$-semimodule in exactly one way.) (props. 4.4, 4.5, & 4.6)

Let $\mathbb{Z}_+$ be the semiring of positive integers under the usual operations of addition and multiplication. $\mathbb{Z}_+$ is initial in the category of semirings: for any semiring S, there is exactly one homomorphism from $\mathbb{Z}_+$ to S. Therefore, a semialgebra over $\mathbb{Z}_+$ is just a semiring, and a semimodule over $\mathbb{Z}_+$ is just a commutative semigroup. This gives us the following hierarchy of notions:

- A semialgebra over $\mathbb{Z}_+$ is a semiring.
- A semialgebra over $\mathbb{Z}$ is a regular semiring.
- An algebra over $\mathbb{Z}$ is a ring.
- A semimodule over $\mathbb{Z}_+$ is a commutative semigroup.
- A semimodule over $\mathbb{Z}$ is an RCS.
- A module over $\mathbb{Z}$ is an abelian group.

Intuitively, RCSs are a natural answer to the question "what lies between commutative semigroups and abelian groups?" and regular semirings are a natural answer to "what lies between semirings and rings?"

I find it likely that the classification of RCSs in terms of abelian groups given in section 3 could be extended into a classification of R-semimodules in terms of R-modules, where R is any commutative ring. In particular, I conjecture that just as every RCS can be constructed from a semilattice-indexed diagram of abelian groups and group homomorphisms, every R-semimodule can be constructed from a semilattice-indexed diagram of R-modules and R-linear maps. I may prove this in a future article.