Enumerating finite semirings

J. D. Mitchell and P. Ragavan

July 1, 2025

Abstract

In this short note we count the finite semirings up to isomorphism and up to anti-isomorphism for some small values of n; for which we utilise the existing library of small semigroups in the GAP [14] package Smallsemi [12].

1 Introduction

Enumeration of algebra and combinatorial structures of finite order up to isomorphism is a classical topic. Among the algebraic structures considered are groups [10], rings [8, 11, 13, 15], near-rings [7, 9], semigroups [5], monoids [4], inverse semigroups [2], loops [6], quasi-groups [3], functional digraphs [1] (or mono-unary algebras to some) and many more too numerous to mention. In this short note we count the number of finite semirings up to isomorphism and up to isomorphism and anti-isomorphism for $n \leq 6$. We also count several special classes of semirings for (slightly) larger values of n.

This short note was initiated by an email from M. Volkov to the first author in February of 2025 asking if it was possible to verify with GAP [14] that the number of ai-semirings up to isomorphism with 4 elements is 866. After some initial missteps it was relatively straightforward to verify that this number is correct, by using the library of small semigroups in the GAP [14] package Smallsemi [12]. This short note arose out from these first steps. In contrast to groups or rings, where the numbers of non-isomorphic objects of order n is known for relatively large values of n, the number of semigroups of order 11 (up to isomorphism) is not known exactly. Given that 99.4% of the semigroups of order 8 are 3-nilpotent, that the number of 3-nilpotent semigroups of order 11 is approximately 10^{26} [**<empty citation>**], this number is likely close to the exact value; see also [**<empty citation>**]. Perhaps unsurprisingly, from the perspective of counting up to isomorphism, it seems that semirings have more in common with semigroups than with rings or groups. Roughly speaking, rings and groups are highly structured, providing strong constraints that enable their enumeration. On the other hand, semigroups, and seemingly semirings also, are less structured, more numerous, and consequently harder to enumerate.

We begin with the definition of a semiring; this originates in [**<empty citation>**] and was intended as a generalisation of the notion of a ring.

Definition 1.1 (Semiring)**.** A *semiring* is a set S equipped with two binary operations $+$ and $\times$ such that:

(a) $(S, +)$ is a commutative semigroup ($(x + y) + z = x + (y + z)$ and $x + y = y + x$ for all $x, y, z \in S$);
(b) $(S, \times)$ is a semigroup ($x \times (y \times z) = (x \times y) \times z$ for all $x, y, z \in S$); and
(c) multiplication $\times$ distributes over addition $+$ ($x \times (y + z) = (x \times y) + (x \times z)$ and $(y + z) \times x = (y \times x) + (z \times x)$ for all $x, y, z \in S$).

In this short note we are concerned with counting semirings up to isomorphism, and so our next definition is that of an isomorphism.

Definition 1.2 (Semiring isomorphism)**.** We say that two semirings $(S, +, \times)$ and $(S, \oplus, \otimes)$ are *isomorphic* if there exists a bijection $\phi : S \to S$ which is simultaneously a semigroup isomorphism from $(S, +)$ to $(S, \oplus)$ and from $(S, \times)$ to $(S, \otimes)$. We refer to ϕ as a *(semiring) isomorphism*.

If $(+, \times) = (\oplus, \otimes)$ in Definition 1.2, then the semiring isomorphism ϕ is called an *automorphism*. The group of all automorphisms of a semiring S is denoted by $\mathrm{Aut}(S)$. Since a semiring is comprised of two semigroups, enumerating semirings is equivalent to enumerating those pairs consisting of an additive semigroup $(S, +)$ and a multiplicative semigroup $(S, \times)$ such that $\times$ distributes over $+$. The next theorem indicates which $(S, \times)$ we should consider for each of the additive semigroups $(S, +)$.

We denote the symmetric group on the set S by $\mathrm{Sym}(S)$. If $\sigma \in \mathrm{Sym}(S)$ and $\cdot : S \times S \to S$ is a binary operation, then we define the binary operation $\cdot^{\sigma} : S \times S \to S$ by

$$x \cdot^{\sigma} y = ((x)\sigma^{-1} \cdot (y)\sigma^{-1})\sigma. \tag{1}$$

It is straightforward to verify that (1) is a (right group) action of $\mathrm{Sym}(S)$ on the set of all binary operations on S. Clearly if $\cdot$ is associative, then so too is $\cdot^{\sigma}$ for every $\sigma \in \mathrm{Sym}(S)$. The group of automorphisms $\mathrm{Aut}(S, \cdot)$ of a semigroup $(S, \cdot)$ coincides with the stabiliser of the operation $\cdot$ under the action of $\mathrm{Sym}(S)$ defined in (1).

Recall that if H and K are subgroups of a group G, then the *double cosets* $H\backslash G/K$ are the sets of the form $\{hgk \mid h \in H, k \in K\}$ for $g \in G$. The next theorem is key to our approach for counting semirings.

Theorem 1.3. *Let $(S, +)$ be a commutative semigroup, let $(S, \times)$ be a semigroup, and let $\sigma, \tau \in \mathrm{Sym}(S)$ be such that $(S, +, \times^{\sigma})$ and $(S, +, \times^{\tau})$ are semirings. Then $(S, +, \times^{\sigma})$ and $(S, +, \times^{\tau})$ are isomorphic if and only if σ and τ belong to the same double coset of $\mathrm{Aut}(S, \times)\backslash \mathrm{Sym}(S)/ \mathrm{Aut}(S, +)$.*

Proof. ($\Rightarrow$) Suppose that ϕ is a semiring isomorphism from $(S, +, \times^{\sigma})$ to $(S, +, \times^{\tau})$. Then $\phi \in \mathrm{Aut}(S, +)$ and $(x \times^{\sigma} y)\phi = (x)\phi \times^{\tau} (y)\phi$ for all $x, y \in S$. It follows that

$$((x)\sigma^{-1} \times (y)\sigma^{-1})\sigma\phi\tau^{-1} = (x \times^{\sigma} y)\phi\tau^{-1} = ((x)\phi \times^{\tau} (y)\phi)\tau^{-1} = (x)\phi\tau^{-1} \times (y)\phi\tau^{-1}.$$

If we set $\gamma = \sigma\phi\tau^{-1}$, $p = (x)\sigma^{-1}$, and $q = (y)\sigma^{-1}$, then $(p \times q)\gamma = (p)\gamma \times (q)\gamma$ and so $\gamma, \gamma^{-1} \in \mathrm{Aut}(S, \times)$. Rearranging we obtain $\tau = \gamma^{-1}\sigma\phi$. Since $\phi \in \mathrm{Aut}(S, +)$, we conclude that τ and σ lie in the same double coset of $\mathrm{Aut}(S, \times)\backslash \mathrm{Sym}(S)/ \mathrm{Aut}(S, +)$.

($\Leftarrow$) Suppose that σ and τ are in the same double coset of $\mathrm{Aut}(S, +)\backslash \mathrm{Sym}(S)/ \mathrm{Aut}(S, \times)$. Then there exists $\alpha \in \mathrm{Aut}(S, \times)$ and $\beta \in \mathrm{Aut}(S, +)$ such that $\tau = \alpha\sigma\beta$.

We will show that β is a semiring isomorphism from $(S, +, \times^{\sigma})$ to $(S, +, \times^{\tau})$. Since $\beta \in \mathrm{Aut}(S, +)$, it suffices to show that β is an isomorphism from $(S, \times^{\sigma})$ and $(S, \times^{\tau})$:

$$\begin{aligned}(x \times^{\sigma} y)\beta &= (x\sigma^{-1} \times y\sigma^{-1})\sigma\beta = (x\sigma^{-1} \times y\sigma^{-1})\alpha^{-1}\tau = (x\sigma^{-1}\alpha^{-1} \times y\sigma^{-1}\alpha^{-1})\tau \qquad && \alpha^{-1} \in \mathrm{Aut}(S, \times)\\ &= (x\beta\tau^{-1} \times y\beta\tau^{-1})\tau = (x\beta \times^{\tau} y\beta). && \square\end{aligned}$$

If $(S, \times)$ and $(S, \otimes)$ are semigroups, then $(S, \times)$ is said to be *anti-isomorphic* to $(S, \otimes)$ if there exists a bijection $\phi : S \to S$ such that $(x \times y)\phi = y \otimes x$ for all $x, y \in S$. The bijection ϕ is referred to as an *anti-isomorphism*. Similarly, using the obvious analogue of Definition 1.2, we can define anti-isomorphic semigroups. It is routine to adapt the proof of Definition 1.3 to prove the following.

Corollary 1.4. *Let A be a commutative semigroup and M be a semigroup, such that A and M are both defined on the same underlying set S. For any permutation $\sigma \in \mathrm{Sym}(S)$, let M^{σ} denote the semigroup obtained by permuting M via σ. Suppose that for two permutations $\sigma, \tau \in \mathrm{Sym}(S)$, the pairs (A, M^{σ}) and (A, M^{τ}) both form semirings. Then, the following statements are equivalent:*

(a) *(A, M^{σ}) and (A, M^{τ}) are equivalent, i.e. isomorphic or anti-isomorphic.*

(b) *σ and τ lie in the same double coset of $\mathrm{Aut}(A)\backslash \mathrm{Sym}(S)/ \mathrm{Aut}^{*}(M)$.*

where $\mathrm{Aut}^{*}(M)$ denotes the group of automorphisms and anti-automorphisms of M.

2 Tables of results

It follows from Definition 1.3 and Definition 1.4 that to enumerate the semirings on a set S up to isomorphism (or up to isomorphism and anti-isomorphism) it suffices to consider every commutative semigroup $(S, +)$ and semigroup $(S, \times)$ and to compute representatives of the double cosets $\mathrm{Aut}(S, \times)\backslash \mathrm{Sym}(S)/ \mathrm{Aut}(S, +)$. The semigroups up to isomorphism are available in SMALLSEMI [12]. Since S is small, it is relatively straightforward to can compute $\mathrm{Aut}(S, \times)$ and $\mathrm{Aut}(S, +)$. GAP [14] contains functionality for computing double coset representatives based on [**<empty citation>**]. This is the approach implemented by the authors of the current paper in the GAP [14] package `semirings` to compute the numbers in this section.

Definition 2.1 (ai-semiring)**.** The prefix 'ai' refers to *additive idempotence*. For instance, an ai-semiring S is a semiring such that the additive reduct is idempotent, i.e. it satisfies $a + a = a$ for all $a \in S$.

Definition 2.2. A *rng* is a ring without the requirement for multiplicative identity. Maintaining the language from Definition 1.1, this may be thought of as the pair (A, M) where A is an abelian group and M is a semigroup.

Definition 2.3. A *rig* S is a ring without the requirement for negatives (additive inverses) such that

$$0 \cdot a = 0 \qquad \forall a \in S, \tag{2}$$

where 0 denotes the additive identity in S.

Note that although generally in a ring, Property (2) follows directly from the axioms, this might not hold if we do not have negatives, and so is instead specified explicitly as an axiom.

As above, this may be thought of as the pair (A, M) where A is a commutative monoid and M is a monoid. In fact, many authors use the term 'rig' to refer to what we have defined as a semiring.

Definition 2.4. A *rg* S is a ring without the requirement for negatives or multiplicative identity, such that

$$0 \cdot a = 0 \qquad \forall a \in S,$$

where 0 denotes the additive identity in S.

The reasoning for this additional axiom is as in Definition 2.3. As above, this may be thought of as the pair (A, M) where A is a commutative monoid and M is a semigroup. The term 'rg' is very non-standard in the literature.

The semiring-like structures that can be counted using the `aisemirings` package are:

- Semirings
- Semirings with one
- Ai-semirings
- Ai-semirings with one
- Rigs
- Ai-rigs
- Rgs
- Ai-rgs
- Rngs
- Rings

For instance, one could count the number of semirings with n elements up to isomorphism using `NrSemirings(n)` or up to equivalence using `NrSemirings(n, true)`. `AllSemirings` could be used to enumerate these objects. Functions for the other objects mentioned above are constructed similarly. Using the helper function `SETUPFINDER`, the package could also easily be used to count/enumerate any object which is a semiring with additional constraints, as long as the sets of valid additive and multiplicative reducts are expressible as families of semigroups. With a little more effort, it would be possible to count semirings for arbitrary sets of valid additive and multiplicative reducts.

The algorithm used to count these objects up to isomorphism is fairly rudimentary and is based on Theorem 1.3. As the condition given by this theorem is precise, we can make use of the `smallsemi` package in GAP to loop over possible semirings (A, M) in a minimal way, such that no two semirings yielded by this process can be isomorphic.

Similarly, we can count semirings up to equivalence by using the condition given in Corollary 1.4, again in a minimal way.

Below are some tables of results for the aforementioned structures. As far as we know, no results are published the number of any of these structures up to equivalence. For results up to isomorphism, those that have not been previously published (as far as we know) are marked '†'. Results that we are in the process of computing are marked '?'. As a sanity check, various results that are already published are available at Peter Jipsen's Mathematical Structures Library, though he makes use of different naming conventions[1].

n	up to isomorphism	up to isomorphism + anti-isomorphism
1	1	1
2	10	9
3	132	106
4	2,341	1,713
5	57,427†	38,247
6	7,571,579†	4,102,358

Table 1: Numbers of semirings with n elements up to isomorphism and up to isomorphism or anti-isomorphism. See Jipsen's library for $n \leq 4$ up to isomorphism.

These tables are merely a sample of the results that can be obtained using the `semirings` package.

[1] Note that Jipsen's page for "semirings with one", seems to be mistitled and actually provides results for ai-semirings with one (which can be counted using the `ai-semirings` package!). This is not a difference in naming convention, but seems to just be a mistake. As far as we know, all results in Table 5 are unpublished.

n	up to isomorphism	up to isomorphism + anti-isomorphism
1	1	1
2	6	5
3	61	45
4	866	581
5	15,751†	9,750
6	354,409†	205,744
7	9,908,909†	5,470,437

Table 2: Numbers of ai-semirings with n elements up to isomorphism and up to isomorphism or anti-isomorphism. See Jipsen's library for $n \leq 4$ up to isomorphism.

n	up to isomorphism	up to isomorphism + anti-isomorphism
1	1	1
2	2	2
3	6	6
4	40	38
5	295	262
6	3,246	2,681
7	59,314†	43,331

Table 3: Numbers of rigs with n elements up to isomorphism and up to isomorphism or anti-isomorphism. See Jipsen's library for $n \leq 6$ up to isomorphism.

References

[1] O. F. I. (2025). *Number of functional digraphs (digraphs of functions on n nodes where every node has outdegree 1 and loops of length 1 are forbidden), Entry A001373 in The On-Line Encyclopedia of Integer Sequences.*

[2] O. F. I. (2025). *Number of inverse semigroups of order n, considered to be equivalent when they are isomorphic or anti-isomorphic (by reversal of the operator), Entry A001428 in The On-Line Encyclopedia of Integer Sequences.*

[3] O. F. I. (2025). *Number of Latin squares of order n; or labeled quasigroups, Entry A002860 in The On-Line Encyclopedia of Integer Sequences.*

[4] O. F. I. (2025). *Number of nonisomorphic monoids (semigroups with identity) of order n, Entry A058129 in The On-Line Encyclopedia of Integer Sequences.*

[5] O. F. I. (2025). *Number of nonisomorphic semigroups of order n, Entry A027851 in The On-Line Encyclopedia of Integer Sequences.*

[6] O. F. I. (2025). *Number of reduced Latin squares of order n; also number of labeled loops (quasigroups with an identity element) with a fixed identity element, Entry A000315 in The On-Line Encyclopedia of Integer Sequences.*

[7] O. F. I. (2025). *The number of near-rings with n elements, Entry A305858 in The On-Line Encyclopedia of Integer Sequences.*

[8] O. F. I. (2025). *The number of rings with n elements, Entry A027623 in The On-Line Encyclopedia of Integer Sequences.*

[9] E. Aichinger et al. *SONATA, System of nearrings and their applications, Version 2.9.6.* Refereed GAP package. Dec. 2022.

[10] H. U. BESCHE, B. EICK, and E. A. O'BRIEN. "A MILLENNIUM PROJECT: CONSTRUCTING SMALL GROUPS". In: *International Journal of Algebra and Computation* 12.05 (Oct. 2002), pp. 623–644. ISSN: 1793-6500. DOI: 10.1142/s0218196702001115. URL: http://dx.doi.org/10.1142/S0218196702001115.

[11] S. R. Blackburn and K. R. McLean. "The enumeration of finite rings". In: *Journal of the London Mathematical Society* 106.4 (July 2022), pp. 3240–3262. ISSN: 1469-7750. DOI: 10.1112/jlms.12661. URL: http://dx.doi.org/10.1112/jlms.12661.

[12] A. Distler and J. Mitchell. *Smallsemi, A library of small semigroups, Version 0.7.2.* GAP package. Feb. 2025.

n	up to isomorphism	up to isomorphism + anti-isomorphism
1	1	1
2	1	1
3	3	3
4	20	18
5	149	125
6	1,488	1,150
7	18,554	13,171
8	295,292†	116,274

Table 4: Numbers of ai-rigs with n elements up to isomorphism and up to isomorphism or anti-isomorphism. See Jipsen's library for $n \leq 7$ up to isomorphism.

n	up to isomorphism	up to isomorphism + anti-isomorphism
1	1	1
2	4	4
3	22	21
4	169	155
5	1,819	1,561
6	41,104	30,112
7	?	?

Table 5: Numbers of semirings with one (unital semirings) with n elements up to isomorphism and up to isomorphism or anti-isomorphism.

[13] B. Fine. "Classification of Finite Rings of Order p^2". In: *Mathematics Magazine* 66.4 (Oct. 1993), p. 248. ISSN: 0025-570X. DOI: 10.2307/2690742. URL: http://dx.doi.org/10.2307/2690742.

[14] *GAP – Groups, Algorithms, and Programming, Version 4.14.0*. The GAP Group. 2024. URL: %5Curl%7Bhttps://www.gap-system.org%7D.

[15] R. L. Kruse and D. T. Price. "Enumerating Finite Rings". In: *Journal of the London Mathematical Society* s2-2.1 (Jan. 1970), pp. 149–159. ISSN: 0024-6107. DOI: 10.1112/jlms/s2-2.1.149. URL: http://dx.doi.org/10.1112/jlms/s2-2.1.149.