

# INTRODUCTION TO SEMIGROUPS AND MONOIDS

PETE L. CLARK

We give here some basic definitions and very basic results concerning semigroups and monoids. Aside from the mathematical maturity necessary to follow the somewhat Bourbakistic expository style, our presentation makes very few demands on the reader. It would, for instance, be possible (we do not claim it is advisable) for the reader to learn the definition of a group as a certain nice kind of monoid.

To be frank, most of the material we include here is not inherently fascinating. On the other hand, it is also quite easy, and knowing it is often helpful and at times indispensable in the study of modern mathematics. Indeed these notes were originally written to provide background material for some of our other expositions, especially [Commutative Algebra] and [Quadratic Forms].

I had the good fortune to be taught this material at the very beginning of my algebraic training, in an undergraduate algebra course given by Prof. Arunas Liulevicius at the University of Chicago in the fall of 1995. Since then I have come to realize how unusual it is to receive an explicit treatment of this simple and useful material at any level. I know many working mathematicians who let loose a smirk or giggle when they hear the word “monoid”. What’s so funny?

## 1. INTRODUCTION

### 1.1. Absolute Basics.

A **semigroup**  $M$  is a **nonempty**<sup>1</sup> set equipped with a binary operation  $\cdot$ , which is required (only!) to be associative.

An element  $e$  of a semigroup  $M$  is said to be an **identity** if for all  $x \in M$ ,  $ex = xe = x$ .

**Proposition 1.** *A semigroup can have at most one identity.*

Proof: If  $e$  and  $e'$  are both identities, then  $e = e \cdot e' = e'$ .

Definition: A **monoid** is a semigroup with an identity element. By Proposition 1, the identity element is unique, and we shall generally denote it by 1.

A semigroup  $M$  is **commutative** if  $x \cdot y = y \cdot x$  for all  $x, y \in M$ .

Some basic examples: The integers, the rational numbers, the real numbers and the complex numbers are all commutative monoids under addition. But these all have additional structure, so are not ideal examples.

---

<sup>1</sup>Many authors would allow the empty semigroup. It is clear what we are missing out on by excluding the empty set as a semigroup (precisely one thing: nothing), so it is nothing to get worked up about either way.

The subset  $\{0\}$  of any of these guys is a semigroup, called **trivial**. The binary operation is that which is inherited from  $\mathbb{Z}$ ; alternately, observe that a one element set  $\{x\}$  has a unique binary operation:  $x \cdot x = \textit{guess what?}$ .

The structure  $(\mathbb{N}, +)$  of natural numbers (i.e., non-negative integers) forms a commutative monoid under addition. The structure  $(\mathbb{Z}^+, \cdot)$  of positive integers forms a commutative monoid under multiplication.

For an example of a semigroup which is not a monoid, take any nontrivial monoid and remove the identity element! (This does require some small verification: check and see for yourself.) Or take the integers greater than or equal to 17. In fact a subset  $S \subset \mathbb{N}$  such that (i)  $\mathbb{N} \setminus S$  is finite and (ii)  $S + S \subset S$  is called a **numerical semigroup**. Take a moment and find some more examples of numerical semigroups. This is already a very interesting class of examples!

Let  $S$  be a nonempty set and  $0$  an element of  $S$ . We can define a semigroup by decreeing  $x \cdot y = 0$  for all  $x, y \in S$ . Such a semigroup is called **null**.

For a noncommutative example, consider the collection of all **binary strings**: an element is a finite ordered sequence of 0's and 1's. The binary operation is just concatenation: e.g.  $1011 \cdot 001001 = 1011001001$ . Is there an identity? The answer is yes if(f) we allow the "empty string." We could of course do a similar construction starting with an arbitrary set  $S$  of symbols instead of  $\{0, 1\}$ . If we took instead  $S = \{1\}$  then we have identities like  $111 \cdot 111111 = 11111111$ , which we might as well abbreviate to  $3 + 5 = 8$ . In other words, in this case we get back the natural numbers under addition (or the positive integers under addition if you take out the empty string.) The monoid of all finite strings of elements (including the empty string) from a set  $S$  is called the **free monoid** on  $S$ . At the moment, all we wanted to do was give an interesting example. We will return to it later.

Here is a stranger example. For any nonempty set  $S$  we can define two semigroups  $L(S)$  and  $R(S)$  on  $S$ . For  $L(S)$ , the binary operation is  $x \cdot y = x$ , and for  $R(S)$  the operation is  $x \cdot y = y$ . As long as  $S$  has more than one element,  $L(S)$  and  $R(S)$  are noncommutative semigroups without identity.

More generally, if  $S$  is any semigroup, one can define the **opposite** semigroup  $S^{op}$  by  $x \bullet y := y \cdot x$ . For instance,  $L(S)$  and  $R(S)$  are opposite semigroups.

If  $M$  and  $N$  are semigroups, then a map  $f : M \rightarrow N$  is a **semi-homomorphism** of semigroups if  $f(m_1 \cdot m_2) = f(m_1) \cdot f(m_2)$  for all  $m_1, m_2 \in M$ .

A semi-homomorphism  $f : M \rightarrow N$  is a **homomorphism** if every identity of  $M$  gets mapped to an identity of  $N$ . In other words, if  $M$  has no identity, every semi-homomorphism is a homomorphism, whereas if  $M$  has an identity, we are requiring that  $N$  has an identity and that  $f(1) = 1$ .

The distinction between semi-homomorphisms and homomorphisms may not be standard,<sup>2</sup> but it seems useful: it warns us away from considering maps with  $f(1) \neq 1$ , which seems to simplify things without missing out on much.

Exercise 1.1:

a) Exhibit a semi-homomorphism of semigroups which is not a homomorphism.

<sup>2</sup>That is to say, I made it up, but, like many things in mathematics which are made up by one person for some reasonable purpose, it may well be that others have done the same.

- b) Show that any surjective semi-homomorphism of monoids is a homomorphism.  
 c) Show that a semi-homomorphism (resp. a homomorphism) of semi-groups is an isomorphism iff it is bijective.

Exercise 1.2:

- a) Show that two null semigroups are isomorphic iff they have the same cardinality.  
 b) Let  $S$  be a set with  $|S| > 1$ . Show that  $L(S)$  and  $R(S)$  are not isomorphic.

A **subsemigroup**  $S$  of a semigroup  $M$  is a nonempty subset of  $M$  such that  $S \cdot S \subset S$ , i.e., such that  $x, y \in S$  implies  $xy \in S$ . A **submonoid**  $N$  of a monoid  $M$  is a subsemigroup  $N$  which contains the identity  $1$  of  $M$ .

Exercise 1.3: Exhibit a monoid  $M$  and a subsemigroup  $N$  such that  $N$  is a monoid, but  $N$  is not a submonoid of  $M$ .

In other words, this terminology partially goes against our previous convention: if  $S$  is a subsemigroup of  $T$ , the inclusion map might only be a semi-homomorphism. But the alternatives (e.g. semisubsemigroup) seem worse.

## 1.2. Adjunction of identities and absorbing elements.

Let  $M \subset \mathbb{N}$  be a numerical semigroup. It is a monoid iff it contains 0. But if it doesn't contain 0, it is easy to see that  $\{0\} \cup M$  is a submonoid of  $\mathbb{N}$ . Similarly, starting with the semigroup of nonempty binary strings, we can get a monoid by simply adjoining an empty string  $e$ . Notice that in either case, the identity was just some added symbol  $e$  which satisfies  $e \cdot e = e$  and  $e \cdot m = m \cdot e = m$  for each element  $m$ . Indeed:

**Proposition 2.** *Let  $M$  be a semigroup, and  $e$  be a formal symbol – all that matters is that  $e$  is **not** an element of  $M$  – and put  $M^e := M \coprod \{e\}$ . If we extend the binary operation on  $M$  to  $M^e$  by putting  $e \cdot e = e$ ,  $e \cdot m = m \cdot e = m$  for all  $m \in M$ , then  $M^e$  is a monoid with identity element  $e$ .*

Exercise 1.4: Prove Proposition 2.

Warning: Proposition 2 can be applied even when  $M$  already has an identity element  $1$ , giving a monoid  $M^e$  in which the old identity element  $1$  is no longer an identity, since  $1 \cdot e = 1 \neq e$ . (Note that if  $M$  is a monoid, the canonical map  $M \hookrightarrow M^e$  is a semi-homomorphism which is *not* a homomorphism.) Thus if we wish to add an identity element if, and only if, there is not one already present, we need a new notation for this: we define  $M^1$  to be  $M$  if  $M$  has an identity and  $M^e$  if it does not. Denote by  $\iota$  the obvious embedding  $M \hookrightarrow M^1$ .

**Proposition 3.** *Let  $f : M \rightarrow N$  be a homomorphism and suppose that  $N$  is a monoid. Then there exists a unique monoid homomorphism  $F : M^1 \rightarrow N$  such that  $f = F \circ \iota$ .*

Proof: If  $M = M^1$  the statement is vacuous, and if  $M^1 = M \coprod \{1\}$ , the unique extension is the one which sends  $1 \mapsto 1$ .

We note that this shows that  $M \mapsto M^1$  is a **monoidal completion** functor in

the sense of universal algebra: i.e., it is the left-adjoint to the forgetful functor from the category of monoids (with monoid homomorphisms) to semigroups (with homomorphisms). We also note that this would not be true if we allowed semi-homomorphisms.

An **absorbing element** in a semigroup  $M$  is an element  $x \in M$  such that for all  $y \in M$ ,  $xy = yx = x$ . We say that a semigroup is a **nulloid** if it has an absorbing element.

**Proposition 4.** *A semigroup has at most one absorbing element.*

Exercise 1.5: Prove Proposition 4.

For example, the monoid  $(\mathbb{Z}, \cdot)$  of integers under multiplication is a nulloid: it has absorbing element 0. More generally if  $(R, +, \cdot)$  is an associative algebra, then  $(R, \cdot)$  is a nulloid, in which the additive identity 0 is the absorbing element. For this reason, one generally denotes an absorbing element in a semigroup as 0.

At this point, it should come as no surprise that given any semigroup  $M$ , one can adjoin a formal symbol  $a$  (anything which is not in  $M$  works fine) to get a semigroup structure on  $M_a := M \amalg \{a\}$  in which  $a$  is an absorbing element.

Exercise 1.6: Prove it.

Exercise 1.7: Define a **nullary map**  $f : M \rightarrow N$  to be a semi-homomorphism of semigroups such that any absorbing element of  $M$  gets mapped to an absorbing element of  $N$ . Define  $M^0$  in an analogous way to  $M^1$  and show that  $\iota : M \hookrightarrow M^0$  is universal for nullary maps from a semigroup to a nulloid. In other words,  $M \mapsto M^0$  is a **nulloidal completion**.

Exercise 1.8: Let  $M$  be a semigroup. Show that  $M$  is commutative  $\iff M^e$  is commutative  $\iff M^a$  is commutative.

The constructions  $M \mapsto M^e$  and  $M \mapsto M^a$  are compatible in the following sense:

**Proposition 5.** *Let  $M$  be a semigroup.*

- a) *If 1 is an identity of  $M$ , then 1 is an identity of  $M^a$ .*
- b) *If 0 is an absorbing element of  $M$ , then 0 is an absorbing element of  $M^e$ .*

Exercise 1.9: Prove Proposition 5.

By iterating these two adjunctions, we get some further examples of finite semigroups. In particular:

Let  $E(1)$  be a one-element monoid. For  $n \in \mathbb{Z}^+$ , recursively define  $E(n+1) = E(n)^e$ . Evidently  $E(n)$  is a commutative monoid of order  $n$ .

**Proposition 6.** *The monoid  $E(n)$  is isomorphic to the set  $[1, n]$  of positive integers from 1 to  $n$  with  $a \cdot b := \max(a, b)$ . The element  $n$  is absorbing and the element 1 is an identity.*

Exercise 1.10: Prove Proposition 6.

Exercise 1.11: Let  $A(1) = E(1)$ . For  $n \in \mathbb{Z}^+$ , recursively define  $A(n+1) = A(n)^a$ . Give a description of  $A(n)$  similar to that of Proposition 6.

### 1.3. Semigroups of order two.

Let  $n$  be a positive integer and  $M$  be a set with  $n$  elements. Let us investigate the various nonisomorphic semigroup structures on  $M$  for (very) small  $n$ .

Clearly if  $n = 1$  there is a unique semigroup structure: if  $M = \{x\}$  then  $x \cdot x = x$ . We call any semigroup of cardinality one **trivial**: obviously there is exactly one trivial semigroup, up to (unique!) isomorphism. Note that in a trivial semigroup the unique element is both an identity and absorbing. It is easy to see that conversely, any semigroup possessing both a 0 and a 1 with  $0 = 1$  is trivial.

Suppose  $n = 2$  and write  $M = \{x, y\}$ . Suppose first that  $M$  has an identity, which (up to relabelling) we may assume is  $x$ . Then we must have  $x^2 = x$ ,  $xy = yx = x$ , so the only thing in doubt is  $y \cdot y = y^2$ . We could of course have  $y^2 = x$  – this gives us the (unique, up to unique isomorphism) group of order 2. The other possibility is  $y^2 = y$ . To see that this works, note that it is in fact  $\{y\}^e$ , i.e., obtained by adjoining an identity to the trivial monoid whose element is called  $y$ . This makes us realize that there is also the semigroup  $\{y\}^a$ , but since  $y$  is an identity in  $\{y\}$ , by Proposition 5  $y$  is also an identity in  $\{y\}^a$ , so up to isomorphism we get nothing new. We have two null semigroups, which are isomorphic. One also has the left semigroup  $L(\{x, y\})$  defined, as above by  $x \cdot x = x \cdot y = x$ ,  $y \cdot x = y \cdot y = y$  and similarly the right semigroup  $R(\{x, y\})$ . These two semigroups are not isomorphic to either of the two previous commutative semigroups, and they are not isomorphic to each other.

We claim there are no other nonisomorphic semigroups on  $\{x, y\}$ . We may assume there is neither an identity nor an absorbing element and, WLOG, that  $xy = x$ .

Case 1a) Suppose  $yx = x$  and  $y^2 = y$ . Then  $y$  is an identity so we are back to the previous examples.

Case 1b) Suppose  $yx = x$  and  $y^2 = x$ . If  $x^2 = x$  then  $x$  is absorbing. If  $x^2 = y$  then  $x(xy) = x^2 = y$  whereas  $(xx)y = y^2 = x$  and the product is not associative.

Case 2a) Suppose  $yx = y$  and  $x^2 = x$ . If  $y^2 = y$  we have the left semigroup. If  $y^2 = x$  then  $(yx)y = x$  whereas  $y(xy) = y$ .

Case 2b) Suppose  $yx = y$  and  $x^2 = y$ . Then  $(xy)x = y$  whereas  $x(yx) = x$ .

So altogether there are 5 isomorphism classes of semigroups of order 2.

Let  $S(n)$  be the number of isomorphism classes of semigroups of order  $n$ . It is known that  $S(3) = 24$ ,  $S(4) = 188$ ,  $S(5) = 1915$ ,  $S(6) = 28634$ ,  $S(7) = 1627672$ .

### 1.4. Direct sums and direct products.

Let  $M$  and  $N$  be two semigroups. Then the Cartesian product  $M \times N$  becomes a semigroup in an obvious way:  $(m_1, n_1) \cdot (m_2, n_2) := (m_1 \cdot m_2, n_1 \cdot n_2)$ . If  $M$  and  $N$  are monoids with identity elements  $e_M$  and  $e_N$ , then  $M \times N$  is a monoid, with identity element  $(e_M, e_N)$ . Exactly the same discussion holds for any finite set  $M_1, \dots, M_N$  of semigroups: we can form the direct sum  $M = \bigoplus_{i=1}^n M_i$ , i.e., the Cartesian product of sets with componentwise operations; if all the  $M_i$ 's are

monoids, so is  $M$ . If we instead have an infinite family  $\{M_i\}_{i \in I}$  of semigroups indexed by a set  $I$ , we can define a semigroup structure on the Cartesian product  $\prod_{i \in I} M_i$  in the obvious way, and if each  $M_i$  is a monoid with identity  $e_i$ , then the product semigroup is a monoid with identity  $(e_i)_{i \in I}$ . If each  $M_i$  is a monoid, we can also define the **direct sum**  $\bigoplus_{i \in I} M_i$ , which is the subset of the direct product  $\prod_{i \in I} M_i$  consisting of all  $I$ -tuples  $(m_i)_{i \in I}$  such that  $m_i = e_i$  for all but finitely many  $i$ . Then we have that  $\bigoplus_{i \in I} M_i$  is a submonoid of the direct product monoid  $\prod_{i \in I} M_i$ .

**Theorem 7.** *The monoid  $(\mathbb{Z}^+, \cdot)$  of positive integers under multiplication is canonically isomorphic to the direct sum of a countably infinite number of copies of the monoid  $(\mathbb{N}, +)$  of natural numbers under addition.*

Exercise 1.12: Prove Theorem 6. Hint: let  $\mathcal{P}$  be the set of all prime numbers: this is a countably infinite set! Show that the Fundamental Theorem of Arithmetic gives an isomorphism  $(\mathbb{Z}^+, \cdot) \xrightarrow{\sim} \bigoplus_{p \in \mathcal{P}} (\mathbb{N}, +)$ .

## 2. RELATIONS WITH GROUPS

An element  $x$  in a monoid  $M$  is said to be **invertible** (or a **unit**) if there exists  $y \in M$  such that  $xy = yx = 1$ . The usual tricks show that for a given  $x$  there can exist at most one such element  $y$ : indeed, if  $xy = yx = xy' = y'x = 1$ , then

$$y' = y' \cdot 1 = y'(xy) = y'xy = (y'x)y = 1 \cdot y = y.$$

Therefore we may speak unambiguously of the **inverse** of an element  $x$  and denote it by  $x^{-1}$ .

Exercise 2.1: Give an example of a monoid  $M$  and an element  $x$  such that there exists  $y$  in  $M$  with  $xy = 1$  but  $yx \neq 1$ .

Obviously the identity is its own inverse. To be sure, no other element of  $M$  needs to have an inverse! For instance, it is clear that in  $(\mathbb{N}, +)$  no positive integer has an additive inverse.

A **group** is a monoid  $M$  in which each element has an inverse.<sup>3</sup>

Exercise 2.2: a) Show that a monoid  $M$  is a group iff: for each  $x \in M$ , the maps

$$x \bullet : M \rightarrow M, y \mapsto xy, \quad \bullet x : M \rightarrow M, y \mapsto yx$$

are both bijections.

b) A nontrivial group has no absorbing element.

c) For any monoid  $M$ , neither  $M^e$  nor  $M^a$  is a group.

Exercise 2.3: Show that any group  $G$  is isomorphic to its opposite group  $M^{\text{op}}$ .

The subclass of groups is in many ways simpler and better behaved than the class

---

<sup>3</sup>Formally speaking, we do not assume any prior knowledge about groups, but informally speaking we do. This would be a somewhat strange way to meet groups for the first time first time, although it was in fact done this way in my first (undergraduate!) abstract algebra course, taught by Arunas Liulevicius.

of all monoids. In this section we explore the following theme: suppose  $M$  is a monoid which is not a group: what can we do about it?

The first observation is that for any monoid  $M$ , the subset  $M^\times$  of all invertible elements is a submonoid of  $M$  in which every element is invertible: i.e.,  $M^\times$  is a group. Evidently  $M^\times$  is the unique largest submonoid of  $M$  which is a group. We call  $M^\times$  the **unit group** of  $M$ .

Unfortunately, as above, for some of the most basic monoids it happens that the unit group is trivial, i.e.,  $M^\times = \{1\}$ . This is the case for  $(\mathbb{N}, +)$  and indeed for the monoid  $F(S)$  of strings on any set  $S$ .

Another idea is to embed a given semigroup  $M$  into a group  $G$ . This is not always possible: e.g. if  $M$  has an absorbing element  $0$  and an element  $x \neq 0$ , then  $0 \cdot x = 0$ , which in a group would imply  $x = 0$ , contradicting the injectivity of  $0 \bullet$ .

Let us introduce new terminology for these injectivity properties: a semigroup  $M$  is said to be **left-cancellative** if for all  $x \in M$ ,  $x \bullet$  is injective, i.e.,  $xy = xz$  implies  $y = z$ . Similarly one says  $M$  is **right-cancellative** if  $x, y, z \in M$ ,  $xy = zy$  implies  $x = z$ , and  $M$  is **cancellative** if it is both left- and right-cancellative.

Example: Let  $S$  be a set with more than one element. The left semigroup  $L(S)$  on  $S$  is right-cancellative but not left-cancellative. The right semigroup  $R(S)$  on  $S$  is left-cancellative but not cancellative.

**Proposition 8.** *Let  $M$  be a finite monoid which is either left-cancellative or right-cancellative. Then  $M$  is a group.*

Proof: Let  $m \in M$ . Suppose first that  $M$  is left-cancellative. Consider the set  $m^i$  of positive powers of  $M$ ; since  $M$  is finite, there must exist  $i < j$  such that  $m^i = m^j$ . Write  $j = i + k$ , so

$$m^i \cdot 1 = m^i = m^j = m^i m^k.$$

Thus by left-cancellation, we have  $1 = m^k$ , so that  $m^{k-1}m = m$ , and  $m^{k-1}$  is an inverse for  $m$ . Since also  $m^j = m^{i+k} = m^{k+i} = m^k m^i$ , the same argument works assuming right-cancellativity. Alternately, the right-cancellative case can be deduced from the left-cancellative case as follows: if  $M$  is right-cancellative,  $M^{\text{op}}$  is left-cancellative, so it is a group, so by Exercise 2.2  $M \cong M^{\text{op}}$ , so  $M$  is a group.

**Theorem 9.** *Let  $M$  be a commutative cancellative semigroup. There exists a certain (canonically defined) commutative group  $G(M)$  and an injective homomorphism of semigroups  $\iota : M \rightarrow G(M)$ .*

Proof: Let  $M$  be a commutative cancellative semigroup, written additively, i.e.,  $x + y$  instead of  $xy$ . The idea is to suitably adapt the construction of the integers from the natural numbers. One way to do this is as follows: let  $\tilde{M} = M \times M$ , i.e., the Cartesian product of  $M$  with itself, with the usual semigroup structure. We wish to interpret a pair  $(x, y)$  as  $x - y$ ; considering this construction in the special case  $M = (\mathbb{N}, +)$ , it is clear that we are not yet done: e.g.  $-1$  is represented by  $(0, 1)$  but also by  $(1, 2)$  and indeed by  $(n, n + 1)$  for any  $n \in \mathbb{N}$ . So we want to define some equivalence relation on these pairs; to figure out which one, suppose

$(x_1, y_1) = (x_2, y_2)$ ; we interpret this as  $x_1 - y_1 = x_2 - y_2$ , and this can be acceptably rewritten as  $x_1 + y_2 = x_2 + y_1$ . Therefore we define  $(x_1, x_2) \sim (y_1, y_2)$  to mean  $x_1 + y_2 = x_2 + y_1$ .

Let us check that this is in fact an equivalence relation – in fact this is the only place in the proof where we need to use the cancellation property. Indeed, the reflexivity and symmetry of  $\sim$  are obvious; as for transitivity: suppose  $(x_1, y_1) \sim (x_1, y_2) \sim (x_3, y_3)$ . Then  $x_1 + y_2 = x_2 + y_1$  and  $x_2 + y_3 = x_3 + y_2$ . Adding these equations we get  $x_1 + x_2 + y_2 + y_3 = x_2 + x_3 + y_1 + y_2$ . Now by assumption we can cancel  $x_2 + y_2$  to get  $x_1 + y_3 = x_3 + y_1$ , i.e.,  $(x_1, y_1) \sim (x_3, y_3)$ . Let us put  $G(M) := \tilde{M} / \sim$ , and denote the equivalence classes by  $[(x, y)]$ . We wish to define

$$[(x_1, y_1)] + [(x_2, y_2)] = [(x_1 + x_2, y_1 + y_2)],$$

but we must check that this is well-defined: if instead we chose  $(x'_1, y'_1) \sim (x_1, y_1)$  and  $(x'_2, y'_2) \sim (x_2, y_2)$ , then  $(x'_1, y'_1) + (x'_2, y'_2) = (x'_1 + x'_2, y'_1 + y'_2)$ , and since

$$x_1 + x_2 + y'_1 + y'_2 = (x_1 + y'_2) + (x_2 + y'_1) = (x'_2 + y_1) + (x'_1 + y_2) = x'_1 + x'_2 + y_1 + y_2,$$

$$(x_1 + x_2, y_1 + y_2) \sim (x'_1 + x'_2, y'_1 + y'_2). \text{ For any } x \in M,$$

$$[(x, x)] + [(y, z)] = [(x + y, x + z)] = [(y, z)],$$

so  $[(x, x)]$  is an identity element. Similarly, since  $[(x, y)] + [(y, x)] = [(x + y, x + y)]$ ,  $[(y, x)]$  is the inverse of  $[(x, y)]$ . And associativity follows simply upon expanding out both sides. Thus we have a commutative group  $G(M)$ .

Finally, define  $G : M \rightarrow G(M)$  by  $G(x) := [(x + x, x)]$ .

Exercise 2.4: Show that  $\iota$  is an injective homomorphism of semigroups.

Since the construction of  $G(M)$  involves passage to the quotient, given a well-understood semigroup  $M$ , it may not be completely obvious “which” abelian group  $G(M)$  is. As we said, the basic example is  $M = (\mathbb{N}, +)$  and it is only reasonable that  $G(M) \cong \mathbb{Z}$ . What happens if  $M \subset \mathbb{N}$  is a numerical semigroup? What if  $M \cong \bigoplus_{i \in I} \mathbb{N}$ ? The following result helps out in this regard.

**Proposition 10.** *Let  $M$  be a commutative cancellative semigroup, and suppose that  $f : M \hookrightarrow H$  is an embedding into any abelian group. If  $M$  does not have an identity, we assume that  $0$  is not in the image of  $\iota$ . Then  $G(M)$  is isomorphic to the subgroup of  $H$  generated by  $\iota(M)$ .*

Proof: The mapping  $\tilde{M} = M \times M \rightarrow H$  given by  $(x, y) \mapsto f(x) - f(y)$  has as its image the subgroup generated by  $f(M)$ . Moreover, since if  $[(x_1, y_1)] = [(x_2, y_2)]$ , then  $x_1 + y_2 = x_2 + y_1$ ,  $f(x_1) + f(y_2) = f(x_2) + f(y_1)$ , so

$$f((x_1, y_1)) = f(x_1) - f(y_1) = f(x_2) - f(y_2) = f((x_2, y_2)),$$

so  $f$  factors through to a map on the quotient  $G(M)$  of  $\tilde{M}$ , which is easily seen to give an isomorphism onto the subgroup generated by  $f$ .

As an application, we apply this to a numerical semigroup  $M \subset \mathbb{N}$  and get  $G(M) = \mathbb{Z}$ . We can apply it to  $\bigoplus_{i \in I} \mathbb{N}$  by embedding it in  $\bigoplus_{i \in I} \mathbb{Z}$  and observing that the subgroup generated by the image of  $\bigoplus_{i \in I} \mathbb{N}$  is all of  $\bigoplus_{i \in I} \mathbb{Z}$ . In other words, the Proposition asserts that  $G(M)$  is the **minimal group** in which  $M$  can be embedded.

Remark: Examples of cancellative noncommutative semigroups which cannot be embedded in groups were constructed by Malcev in 1936. We do not attempt to go into them here.

From Proposition XX it is only a small step to show that  $G : M \rightarrow G(M)$  is universal for homomorphisms from a cancellative commutative semigroup into a group. In other words, given any homomorphism of semigroups  $f : M \rightarrow H$  where  $H$  is a group, there exists a unique group homomorphism  $F : G(M) \rightarrow H$  such that  $f = F \circ G$ . Indeed, the only possible map would be induced by the map  $F : (x, y) \mapsto x - y$  from  $\tilde{M} = M \times M \rightarrow H$ , and an easy computation as above shows that  $F$  descends to give a well-defined homomorphism on  $G(M)$ .

This remark allows us to wonder: suppose  $M$  is a commutative semigroup which is not cancellative. Then there is no embedding from  $M$  into a group, but is there still a group  $G(M)$  and a homomorphism  $G : M \rightarrow G(M)$  into a group  $G(M)$  which is **universal**, i.e., for every homomorphism  $f : M \rightarrow H$  into a group  $H$ , there exists a unique group homomorphism  $F : G(M) \rightarrow H$  such that  $f = F \circ G$ ?

The answer is yes. In fact the proof of Theorem XX goes through if we strengthen the definition of  $\sim$  to:  $(x_1, y_1) \sim (x_2, y_2)$  iff there exists  $z \in M$  such that  $z + x_1 + y_2 = z + x_2 + y_1$ . We ask the reader to verify this and therefore prove the following result:

**Theorem 11.** *Let  $M$  be a commutative semigroup, written additively. Define  $G(M) = M \times M / \sim$ , where  $(x_1, y_1) \sim (x_2, y_2)$  iff there exists  $z \in M$  such that  $x_1 + y_2 + z = x_2 + y_1 + z$ .*

- a) *coordinatewise addition on  $M \times M$  descends to a well-defined operation on  $G(M)$  which makes it into an abelian group.*
- b) *The map  $x \mapsto [(x + x, x)]$  defines a homomorphism  $G : M \rightarrow G(M)$ , which is injective iff  $M$  is cancellative.*
- c) *The pair  $(G(M), G)$  is universal for homomorphisms from a commutative monoid to a commutative group.*

The functor  $G : M \mapsto G(M)$  is called **group completion**.

Exercise 2.5: Suppose that  $M$  is a commutative semigroup with an absorbing element. Show that its group completion  $G(M)$  is the trivial group.

A **semialgebra** is a triple  $(S, +, \cdot)$  consisting of a set  $S$  endowed with two binary operations called  $+$  and  $\cdot$ , such that  $(S, +)$  is a commutative semigroup with identity element called  $0$ ,  $(S, \cdot)$  is a semigroup,  $0$  is an absorbing element for  $(S, \cdot)$ , and for all  $x, y, z \in S$ ,  $x \cdot (y + z) = x \cdot y + x \cdot z$ ,  $(x + y) \cdot z = x \cdot z + y \cdot z$ . If  $(S, \cdot)$  has an identity – which will be denoted by  $1$  – we say  $S$  is a **semiring**.

For example, the natural numbers form a semiring under the usual operations of addition and multiplication, as do the positive integers.

**Proposition 12.** *Suppose that  $(S, +, \cdot)$  is a semialgebra.*

- a) *The binary operation*

$$(x_1, x_2) \cdot (y_1, y_2) := (x_1x_2 + y_1y_2, x_1y_2 + y_1x_2)$$

on  $\tilde{S} = S \times S$  descends to  $G(S)$ .

b) The triple  $(G(S), +, \cdot)$  is an algebra. If  $(S, \cdot)$  has an identity element 1, then  $[(1, 0)]$  is an identity element for  $(G(S), \cdot)$ , giving it the structure of a ring.

Exercise 2.6: Prove it.

Advanced Example: Let  $R$  be a ring. Let  $\tilde{K}(R) := (\mathcal{M}(R), +)$  be the commutative monoid whose underlying set consists of isomorphism classes of finitely generated projective left  $R$ -modules, and with  $M + N = M \oplus N$ . Then the Grothendieck group of this monoid is denoted  $K_0(R)$ , the  $K$ -group of  $R$ . If  $R$  is commutative, then  $\tilde{K}(R)$  becomes a semiring under  $M \cdot N := M \otimes_R R$ : the unit element is the  $R$ -module  $R$ . In this case  $K_0(R)$  becomes a commutative ring. Its group of units is the set of isomorphism classes of rank 1 projective modules, the **Picard group** of  $R$ .

Let  $X$  be a “space”, which here means that we have a notion of what vector bundles on  $X$  are. (There may well be more than one such notion – e.g. real and complex vector bundles on a real manifold. If so, we fix one such notion for the purposes of this problem.) Then we can define  $\tilde{K}(X)$  to be the semiring whose underlying set consists of isomorphism classes of vector bundles on  $V$  on  $X$ , with  $V + W := V \oplus W$  and  $V \cdot W := V \otimes W$ . Then  $K_0(X)$  denotes the Grothendieck group of  $\tilde{K}(X)$ , with its induced structure of a commutative ring. Its group of units is denoted by  $\text{Pic}(X)$  and is identified with the group of isomorphism classes of line bundles. (This recovers the case of commutative rings by taking  $X = \text{Spec } R$ .)

## 2.1. Partial inversion.

Given a commutative semigroup  $M$ , one often wishes to work in a semigroup in which some but not necessarily all of the elements of  $M$  have inverses. It is not difficult to generalize the above constructions to handle this.

First, let us give a precise formulation of the problem via a universal mapping property. If  $M$  is a semigroup, let  $S$  be a subsemigroup. What we want is a semigroup  $M[S^{-1}]$  which comes equipped with a homomorphism  $\iota : M \rightarrow M[S^{-1}]$  which is **universal** for all homomorphisms  $f : M \rightarrow N$  where  $N$  is a monoid and  $f(S) \subset N^\times$ : that is, there exists a unique homomorphism  $F : M[S^{-1}] \rightarrow N$  such that  $f = F \circ \iota$ .

In the case that  $M$  is cancellative, it is easy to see that the semigroup we are looking for is just the subsemigroup of  $G(M)$  generated by the sets of inverses of elements of  $S$ . In this case the map  $\iota : M \rightarrow M[S^{-1}]$  is injective. In the general case we need only modify the construction by replacing  $\tilde{M} = M \times M$  by  $M_S := M \times S$  and define the equivalence relation to be  $(m_1, s_1) \sim (m_2, s_2)$  iff there exists  $m \in M$  such that  $m + m_1 + s_2 = m + m_2 + s_1$ .

Exercise 2.7: Show that the addition operation is well-defined on  $M_S / \sim$  and gives it the structure of a commutative monoid  $M[S^{-1}]$ , in which each element of  $S$  is invertible. Show that there is a natural homomorphism  $M \rightarrow M[S^{-1}]$  which is universal for mappings  $f : M \rightarrow N$ , where  $N$  is a monoid and  $f(S) \subset N^\times$ .

Exercise 2.8: Can you find necessary and sufficient conditions on  $M$  and  $S$  such that  $M[S^{-1}]$  is nontrivial?

Exercise 2.9: Suppose that  $R$  is a commutative ring. A subsemigroup  $S \subset (M, \cdot)$  is called a **multiplicative subset** of  $S$ . Show that the operation  $(r_1, s_1) + (r_2, s_2) := (r_1 s_2 + s_2 r_1, s_1 s_2)$  on  $M_S = S \times R$  descends to the quotient  $R[S^{-1}]$  and gives it the structure of a commutative ring.

b) Formulate a universal property for the ring homomorphism  $R \mapsto R[S^{-1}]$ .

c) Notice that if  $0 \in S$ , then  $R[S^{-1}] = 0$ . Find a necessary and sufficient condition for this to hold.

d) One says that  $R$  is an **integral domain** if  $(R \setminus \{0\}, \cdot)$  is cancellative. Deduce from the general theory that in this case,  $F(R) := R[(R \setminus \{0\})^{-1}]$  is a field, and the map  $R \rightarrow F(R)$  is universal for injective maps from  $R$  into a field.  $F(R)$  is said to be the **field of fractions** of  $R$ .

### 3. IDEALS AND CONGRUENCES

**Most of this section remains to be written.**

In elementary number theory one learns about congruences modulo  $n$ , in particular that the usual operations of addition and multiplication on  $\mathbb{Z}$  are well-defined modulo  $n$ , leading to a finite ring  $\mathbb{Z}/n\mathbb{Z}$ . Later on in abstract algebra one learns to reexpress this: we say that  $\mathbb{Z}/n\mathbb{Z}$  is the quotient ring modulo the ideal  $(n\mathbb{Z})$ .

However, in the context of semigroups, congruences and ideals are related but distinct concepts.

Let  $M$  be a semigroup. A nonempty subset  $S$  of  $M$  is a **left ideal** (resp. **right ideal**) if for all  $s \in S$ ,  $m \in M$ ,  $ms \in S$  (resp.  $sm \in S$ ). An **ideal** is a subset which is both a left and a right ideal.

Example: In the semigroup of positive integers under addition, for any positive integer  $N_0$ , the subset of all positive integers greater than or equal to  $N_0$  is an ideal.

Let  $M$  be a semigroup. An equivalence relation  $\sim$  on  $M$  is said to be **compatible** with the semigroup structure if  $x_1 \sim x_2$ ,  $y_1 \sim y_2$  implies  $x_1 y_1 \sim x_2 y_2$ .

Compatibility is a necessary and sufficient condition for the semigroup operation to be well-defined on the quotient  $M/\sim$ : in other words, we would like to define  $[x_1][y_1] := [x_1 y_1]$ , but for this to make sense we need, for all  $x_2 \sim x_1$ ,  $y_2 \sim y_1$ ,  $[x_1 y_1] = [x_2 y_2]$ , i.e.,  $x_1 y_1 \sim x_2 y_2$ . Therefore a compatible equivalence relation gives rise to a **quotient semigroup**  $M/\sim$  such that the “canonical map”  $x \mapsto [x]$  is a homomorphism of semigroups.

We have already seen examples of this: if  $M$  is a cancellative semigroup, the relation  $(x_1, y_1) \sim (x_2, y_2)$  iff  $x_1 + y_2 = x_2 + y_1$  on  $M \oplus M$  is a compatible equivalence relation; the group  $G(M)$  is precisely the quotient by this relation.

### 4. FREE SEMIGROUPS

**This section has not yet been written.**