Permutation Groups and Transformation Semigroups
Lecture 2: Semigroups

Peter J. Cameron
Permutation Groups summer school, Marienheide
18–22 September 2017

I am assuming that you know what a group is, but I will not make the same assumption about semigroups. This lecture introduces semigroups and transformation semigroups.

1 Basic concepts

We begin with the definitions.

- A *semigroup* is a set S with a binary operation $\circ$ satisfying the *associative law*:
$$a \circ (b \circ c) = (a \circ b) \circ c$$
for all $a, b, c \in S$.
- A *monoid* is a semigroup with an *identity* 1, an element satisfying
$$a \circ 1 = 1 \circ a = a$$
for all $a \in S$.
- A *group* is a monoid with *inverses*, that is, for all $a \in S$ there exists $b \in S$ such that
$$a \circ b = b \circ a = 1.$$

From now on we will write the operation as *juxtaposition*, that is, write ab instead of $a \circ b$, and a^{-1} for the inverse of a.

There is essentially no difference between semigroups and monoids: any monoid is a semigroup, and conversely, to any semigroup we can add an identity without violating the associative law. However, there is a very big difference between semigroups and groups:

Order	1	2	3	4	5	6	7	8
Groups	1	1	1	2	1	2	1	5
Monoids	1	2	7	35	228	2237	31559	1668997
Semigroups	1	5	24	188	1915	28634	1627672	3684030417

A semigroup which will occur often in our discussions is the *full transformation semigroup* $T(\Omega)$ on the set Ω, whose elements are all the maps from Ω to itself, and whose operation is composition. This is the analogue of the symmetric group in semigroup theory. Usually Ω is finite, say $|\Omega| = n$, and we write this semigroup as T_n. As with permutations, we write maps on the right of their arguments, and compose from left to right.

$T(\Omega)$ is a monoid: the identity element is the identity map. It contains the symmetric group $\mathrm{Sym}(\Omega)$, the group of all permutations. Note that $T(\Omega) \setminus \mathrm{Sym}(\Omega)$ is a semigroup.

The order of T_n is $|T_n| = n^n$.

2 Special semigroups

The most interesting semigroups are usually those which are (in some sense) closest to groups.

An element a of a semigroup S is *regular* if there exists $x \in S$ such that $axa = a$. The semigroup S is *regular* if all its elements are regular. Note that a group is regular, since we may choose $x = a^{-1}$.

Regularity is equivalent to a condition which appears formally to be stronger:

Proposition 2.1 *If $a \in S$ is regular, then there exists $b \in S$ such that $aba = a$ and $bab = b$.*

Proof Choose x such that $axa = a$, and set $b = xax$. Then

$$aba = axaxa = axa = a,$$
$$bab = xaxaxax = xaxax = xax = b.$$

Proposition 2.2 *The semigroup T_n is regular.*

Proof Given a map a, choose a preimage s for every t in the image of a, and define x to map t to s if t is in the image of a (arbitrary otherwise).

An *idempotent* in a semigroup S is an element e such that $e^2 = e$. Note that, if $axa = a$, then ax and xa are idempotents. In a group, there is a unique idempotent, the identity. By contrast, it is possible for a non-trivial semigroup to be generated by its idempotents, as we will see later.

Idempotents have played an important role in semigroup theory. One reason for this is that they always exist in a finite semigroup:

Proposition 2.3 *Let S be a finite semigroup, and $a \in S$. Then some power of a is an idempotent.*

Proof Since S is finite, the powers of a are not all distinct: suppose that $a^m = a^{m+r}$ for some $m, r > 0$. Then $a^i = a^{i+tr}$ for all $i \geq m$ and $t \geq 1$; choosing i to be a multiple of r which is at least m, we see that $a^i = a^{2i}$, so a^i is an idempotent.

It follows that a finite monoid with a unique idempotent is a group. For the unique idempotent is the identity; and, if $a^i = 1$, then a has an inverse, namely a^{i-1}.

A semigroup S is an *inverse semigroup* if for each a there is a unique b such that $aba = a$ and $bab = b$. The element b is called the *inverse* of a. Among several other definitions, I menion just one: it is a semigroup S in which, for every $a \in S$, there is an element $a' \in S$ such that

$$(a')' = a, \quad aa'a = a \quad aa'bb' = bb'aa'$$

for all $a, b \in S$. Thus an inverse semigroup is a regular semigroup in which idempotents commute. (For this we need to show that every idempotent has the form aa'.) In an inverse semigroup, we often write a^{-1} for a'.

Proposition 2.4 *Let S be an inverse semigroup.*

(a) Each element of S has a unique inverse.

(b) The idempotents form a semilattice under the order relation $e \leq f$ if $ef = fe = f$.

3 The symmetric inverse semigroup

The most famous inverse semigroup is the *symmetric inverse semigroup* $I(\Omega)$ on the set Ω. Its elements are the *partial bijections* on this set, that is, all bijective

maps $f : X \to Y$, where $X, Y \subseteq \Omega$. We compose elements wherever possible. Thus, if $f : X \to Y$ and $g : A \to B$, then fg is defined on the preimage (under f) of $Y \cap A$, and maps it to the image (under g) of this set. If $f : X \to Y$, then the inverse (as required in the definition of an inverse semigroup) is the inverse function, which maps Y to X: so ff^{-1} is the identity map on X, and $f^{-1}f$ the identity map on Y. If $|\Omega| = n$, we write this semigroup as I_n. Its order is

$$|I_n| = \sum_{k=0}^{n} \binom{n}{k}^2 k!,$$

since, for a map of rank k, there are $\binom{n}{k}$ choices for the domain and the same number for the rank, and $k!$ bijections between them.

Idempotents are just identity maps on subsets, and the semilattice of idempotents is simply the lattice of subsets of the set $\{1, \ldots, n\}$.

The formulae for the orders of the symmetric group ($|S_n| = n!$) and the full transformation semigroup ($|T_n| = n^n$) are simple and well-known. The order of the symmetric inverse semigroup is less familiar: it is sequence A002720 in the On-Line Encyclopedia of Integer Sequences, beginning

$$1, 2, 7, 34, 209, 1546, 13327, 130922, 1441729, 17572114, \ldots$$

There is a natural construction for subsemigroups of $I(\Omega)$ which gives many beautiful examples but has not been much studied.

Suppose that $\mathscr{L}$ is a *meet-semilattice* of subsets of Ω: that is, a set of subsets closed under intersection. Let G be a permutation group on Ω which preserves $\mathscr{L}$. Then the set of all restrictions of elements of G to sets in $\mathscr{L}$ is an inverse semigroup. For let g_1 and g_2 be elements of G, and A_1 and A_2 sets in $\mathscr{L}$; let h_i be the restriction of g_i to A_i. Then h_1h_2 is the restriction of g_1g_2 to $A_1 \cap A_2g^{-1}$, and this set belongs to $\mathscr{L}$, by assumption.

For an example of this construction, take Ω to be a vector space, G the general linear group, and $\mathscr{L}$ the set of subspaces.

4 Analogues of Cayley's theorem

Cayley's Theorem asserts that a group of order n is isomorphic to some subgroup of S_n. The proof is well-known: we take the *Cayley table* of the group G, the matrix (with rows and columns labelled by group elements); each column of the Cayley table (say the column indexed by b) corresponds to a transformation ρ_b of

the set G (taking the row label a to the product ab, the ath element of column b). Then it is straightforward to show that

- ρ_b is a permutation, so that $\rho_b \in S_n$;
- the map $b \mapsto \rho_b$ is one-to-one;
- the map $b \mapsto \rho_b$ is a homomorphism.

So the set $\{\rho_b : b \in G\}$ is a subgroup of S_n isomorphic to G.

This theorem has an important place in the history of group theory. In the nineteenth century, the subject changed from descriptive (the theory of *transformation groups* or *permutation groups*) to axiomatic; Cayley's theorem guarantees that the "new" abstract groups are the same (up to isomorphism) as the "old" permutation groups or subgroups of S_n.

Almost the same is true for semigroups:

Proposition 4.1 *Any semigroup of order n is isomorphic to a subsemigroup of the full transformation semigroup T_{n+1}.*

Proof If we follow the proof of Cayley's theorem, the thing that could go wrong is the second bullet point: the map $b \mapsto \rho_b$ may not be one-to-one. To fix the problem, we first add an identity element to the semigroup, and then follow Cayley's proof. Now, if $\rho_b = \rho_c$ and 1 is the identity, then

$$b = 1b = 1\rho_b = 1\rho_c = 1c = c,$$

so the map $b \mapsto \rho_b$ is one-to-one.

For inverse semigroups, there is a similar representation theorem. The proof is a little more complicated, and is not given here.

Theorem 4.2 (Vagner–Preston Theorem) *Let S be an inverse semigroup of order n. Then S is isomorphic to a sub-semigroup of the symmetric inverse semigroup I_n.*

5 Basics of transformation semigroups

We discuss a few concepts related to transformations and transformation semigroups on a finite domain Ω.

Any map $f : \Omega \to \Omega$ has an *image*

$$\mathrm{Im}(f) = \{xf : x \in \Omega\},$$

and a *kernel*, the equivalence relation $\equiv_f$ defined by

$$x \equiv_f y \Leftrightarrow xf = yf,$$

or the corresponding partition of Ω. (We usually refer to the partition when we speak about the kernel of f, which is denoted $\mathrm{Ker}(f)$.) The *rank* $\mathrm{rank}(f)$ of f is the cardinality of the image, or the number of parts of the kernel.

Under composition, we clearly have

$$\mathrm{rank}(f_1 f_2) \leq \min\{\mathrm{rank}(f_1), \mathrm{rank}(f_2)\},$$

and so the set $S_m = \{f \in S : \mathrm{rank}(f) \leq m\}$ of elements of a transformation semigroup which have rank at most m is itself a transformation semigroup. In general, there is no dual concept; but the set of permutations in S (elements with rank n) is closed under composition, and forms a permutation group (which is the group of units of S), if it happens to be non-empty. The interplay between permutation groups and transformation semigroups is central to these lectures.

Suppose that f_1 and f_2 are transformations of rank r. As we saw, the rank of $f_1 f_2$ is at most r. Equality holds if and only if $\mathrm{Im}(f_1)$ is a *transversal*, or *section*, for $\mathrm{Ker}(f_2)$, in the sense that it contains exactly one point from each part of the partition $\mathrm{Ker}(f_2)$. This combinatorial relation between subsets and partitions is crucial for what follows. We note here one simple consequence.

Proposition 5.1 *Let f be a transformation of Ω, and suppose that $\mathrm{Im}(f)$ is a section for $\mathrm{Ker}(f)$. Then some power of f is an idempotent with rank equal to that of f.*

For the restriction of f to its image is a permutation, and some power of this permutation is the identity.

Question Let G be a finite group. Let S_1 be the transformation semigroup consisting of all *endomorphisms* of G (homomorphisms from G into itself), and S_2 the

inverse semigroup of all *partial isomorphisms* of G (all isomorphisms $H_1 \to H_2$, where $H_1, H_2 \leq G$). Prove that, if G is an abelian group, then $|S_1| = |S_2|$.

I do not know any non-abelian group satisfying this equation. Is this a characterisation of abelian groups?