MATH 433

Applied Algebra

Lecture 23: Semigroups.

Semigroups

Definition. A **semigroup** is a nonempty set S, together with a binary operation $*$, that satisfies the following axioms:

(S1: closure)
for all elements g and h of S, $g * h$ is an element of S;

(S2: associativity)
$(g * h) * k = g * (h * k)$ for all $g, h, k \in S$.

The semigroup $(S, *)$ is said to be a **monoid** if it satisfies an additional axiom:

(S3: existence of identity) there exists an element $e \in S$ such that $e * g = g * e = g$ for all $g \in S$.

Optional useful properties of semigroups:

(S4: cancellation) $g * h_1 = g * h_2$ implies $h_1 = h_2$ and $h_1 * g = h_2 * g$ implies $h_1 = h_2$ for all $g, h_1, h_2 \in S$.

(S5: commutativity) $g * h = h * g$ for all $g, h \in S$.

Examples of semigroups

- Clearly, any group is also a semigroup and a monoid.

- Real numbers $\mathbb{R}$ with multiplication (commutative monoid).

- Positive integers with addition (commutative semigroup with cancellation).

- Positive integers with multiplication (commutative monoid with cancellation).

- $\mathbb{Z}_n$, congruence classes modulo n, with multiplication (commutative monoid).

- Given a nonempty set X, all functions $f : X \to X$ with composition (monoid).

- All injective functions $f : X \to X$ with composition (monoid with left cancellation: $g \circ f_1 = g \circ f_2 \implies f_1 = f_2$).

- All surjective functions $f : X \to X$ with composition (monoid with right cancellation: $f_1 \circ g = f_2 \circ g \implies f_1 = f_2$).

Examples of semigroups

- All $n \times n$ matrices with multiplication (monoid).
- All $n \times n$ matrices with integer entries, with multiplication (monoid).
- Invertible $n \times n$ matrices, with multiplication (group).
- Invertible $n \times n$ matrices with integer entries, with multiplication (monoid with cancellation).
- All subsets of a set X with the operation of union (commutative monoid).
- All subsets of a set X with the operation of intersection (commutative monoid).
- Positive integers with the operation $a * b = \max(a, b)$ (commutative monoid).
- Positive integers with the operation $a * b = \min(a, b)$ (commutative semigroup).

Examples of semigroups

• Given a finite alphabet X, the set X^* of all finite words in X with the operation of concatenation.

If $w_1 = a_1 a_2 \ldots a_n$ and $w_2 = b_1 b_2 \ldots b_k$, then $w_1 w_2 = a_1 a_2 \ldots a_n b_1 b_2 \ldots b_k$. This is a monoid with cancellation. The identity element is the empty word.

• The set $S(X)$ of all automaton transformations over an alphabet X with composition.

Any transducer automaton with the input/output alphabet X generates a transformation $f : X^* \to X^*$ by the rule $f(\text{input-word}) = \text{output-word}$. It turns out that the composition of two transformations generated by finite state automata can also be generated by a finite state automaton.

Powers of an element in a semigroup

Suppose S is a semigroup. Let us use multiplicative notation for the operation on S. The **powers** of an element $g \in S$ are defined inductively:

$$g^1 = g \text{ and } g^{k+1} = g^k g \text{ for every integer } k \geq 1.$$

Theorem Let g be an element of a semigroup G and $r, s \in \mathbb{Z}$, $r, s > 0$. Then **(i)** $g^r g^s = g^{r+s}$, **(ii)** $(g^r)^s = g^{rs}$.

Proof: Both formulas are proved by induction on s.
(i) The base case $s = 1$ follows from the definition: $g^r g^1 = g^r g = g^{r+1}$. The induction step relies on associativity. Assume that $g^r g^s = g^{r+s}$ for some value of s (and all r). Then $g^r g^{s+1} = g^r(g^s g) = (g^r g^s)g = g^{r+s}g = g^{r+(s+1)}$.
(ii) The base case $s = 1$ is trivial: $(g^r)^1 = g^r = g^{r \cdot 1}$. The induction step relies on (i), which has already been proved. Assume that $(g^r)^s = g^{rs}$ for some value of s and all r. Then $(g^r)^{s+1} = (g^r)^s g^r = g^{rs} g^r = g^{rs+r} = g^{r(s+1)}$.

Theorem Any finite semigroup with cancellation is, in fact, a group.

Lemma If S is a finite semigroup with cancellation, then for any $s \in S$ there exists an integer $k \geq 2$ such that $s^k = s$.

Proof: Since S is finite, the sequence $s, s^2, s^3, \ldots$ contains repetitions. Hence $s^k = s^m$ for some k and m such that $k > m \geq 1$. If $m = 1$ then we are done. If $m > 1$ then $s^{m-1}s^{k-m+1} = s^{m-1}s$. After cancellation, $s^{k-m+1} = s$.

Proof of the theorem: Take any $s \in S$. By Lemma, we have $s^k = s$ for some $k \geq 2$. Let us show that $e = s^{k-1}$ is the identity element. Indeed, for any $g \in S$ we have $s^k g = sg$ or, equivalently, $s(eg) = sg$. After cancellation, $eg = g$. Similarly, $ge = g$ for all $g \in S$. Finally, for any $g \in S$ there is $n \geq 2$ such that $g^n = g = ge$. Then $g^{n-1} = e$, which implies that $g^{n-2} = g^{-1}$.

From a semigroup to a group

Question. When a semigroup S can be extended to a group?

Necessary conditions are cancellation laws since they hold in any group. In general, they are not sufficient.

Theorem If S is a commutative semigroup with cancellation, then it can be extended to an abelian group G such that any element $g \in G$ is of the form $g = b^{-1}a$, where $a, b \in S$.

The group G is called the **group of fractions** of the semigroup S.