MATH 433
Applied Algebra

Lecture 22:
Semigroups.
Rings.

Groups

Definition. A **group** is a set G, together with a binary operation $*$, that satisfies the following axioms:

(G1: closure)
for all elements g and h of G, $g * h$ is an element of G;

(G2: associativity)
$(g * h) * k = g * (h * k)$ for all $g, h, k \in G$;

(G3: existence of identity)
there exists an element $e \in G$, called the **identity** (or **unit**) of G, such that $e * g = g * e = g$ for all $g \in G$;

(G4: existence of inverse)
for every $g \in G$ there exists an element $h \in G$, called the **inverse** of g, such that $g * h = h * g = e$.

The group $(G, *)$ is said to be **commutative** (or **Abelian**) if it satisfies an additional axiom:

(G5: commutativity) $g * h = h * g$ for all $g, h \in G$.

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 $g \in S$.

Additional 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

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

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

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

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

• All $n \times n$ matrices with multiplication (monoid).

• Invertible $n \times n$ matrices with integer entries, with multiplication (monoid with cancellation).

• All subsets of a set X with the operation $A * B = A \cup B$ (commutative monoid).

• Positive integers with the operation $a * b = \max(a, b)$ (commutative monoid).

Examples of semigroups

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

If $w_1 = a_1 a_2 \dots a_n$ and $w_2 = b_1 b_2 \dots b_k$, then $w_1 w_2 = a_1 a_2 \dots a_n b_1 b_2 \dots b_k$. 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 is also generated by a finite state automaton.

Theorem Any finite semigroup with cancellation is actually 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 $s, s^2, s^3, \dots$ contains repetitions, i.e., $s^k = s^m$ for some $k > m \geq 1$. If $m = 1$ then we are done. If $m > 1$ then $s^{m-1}s^{k-m+1} = s^{m-1}s$, which implies $s^{k-m+1} = s$.

Proof of the theorem: Take any $s \in S$. By Lemma, we have $s^k = s$ for some $k \geq 2$. Then $e = s^{k-1}$ 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 $g^{n-2} = g^{-1}$.

Rings

Definition. A **ring** is a set R, together with two binary operations usually called **addition** and **multiplication** and denoted accordingly, such that

- R is an Abelian group under addition,
- R is a semigroup under multiplication,
- multiplication distributes over addition.

The complete list of axioms is as follows:

(R1) for all $x, y \in R$, $x + y$ is an element of R;
(R2) $(x + y) + z = x + (y + z)$ for all $x, y, z \in R$;
(R3) there exists an element, denoted 0, in R such that $x + 0 = 0 + x = x$ for all $x \in R$;
(R4) for every $x \in R$ there exists an element, denoted $-x$, in R such that $x + (-x) = (-x) + x = 0$;
(R5) $x + y = y + x$ for all $x, y \in R$;
(R6) for all $x, y \in R$, xy is an element of R;
(R7) $(xy)z = x(yz)$ for all $x, y, z \in R$;
(R8) $x(y+z) = xy+xz$ and $(y+z)x = yx+zx$ for all $x, y, z \in R$.

Examples of rings

In most examples, addition and multiplication are naturally defined and verification of the axioms is straightforward.

- Real numbers $\mathbb{R}$.
- Integers $\mathbb{Z}$.
- $2\mathbb{Z}$: even integers.
- $\mathbb{Z}_n$: congruence classes modulo n.
- $\mathcal{M}_n(\mathbb{R})$: all $n \times n$ matrices with real entries.
- $\mathcal{M}_n(\mathbb{Z})$: all $n \times n$ matrices with integer entries.
- $\mathbb{R}[X]$: polynomials in variable X with real coefficients.
- $\mathbb{R}(X)$: rational functions in variable X with real coefficients.
- All functions $f : \mathbb{R} \to \mathbb{R}$.
- **Zero ring**: any additive Abelian group with trivial multiplication: $xy = 0$ for all x and y.
- Trivial ring $\{0\}$.

Zero-divisors

Theorem Let R be a ring. Then $x0 = 0x = 0$ for all $x \in R$.

Proof: Let $y = x0$. Then $y + y = x0 + x0 = x(0 + 0)$ $= x0 = y$. It follows that $(-y) + y + y = (-y) + y$, hence $y = 0$. Similarly, one shows that $0x = 0$.

A nonzero element x of a ring R is a **left zero-divisor** if $xy = 0$ for another nonzero element $y \in R$. The element y is called a **right zero-divisor**.

Examples. • In the ring $\mathbb{Z}_6$, the zero-divisors are congruence classes $[2]_6$, $[3]_6$, and $[4]_6$, as $[2]_6[3]_6 = [4]_6[3]_6 = [0]_6$.

• In the ring $\mathcal{M}_n(\mathbb{R})$, the zero-divisors (both left and right) are nonzero matrices with zero determinant. For instance,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

• In any zero ring, all nonzero elements are zero-divisors.