MATH 415

Modern Algebra I

Lecture 4: Groups and semigroups. Subgroups.

Groups

Definition. A **group** is a binary structure $(G, *)$ that satisfies the following axioms:

(G0: closure)
for all elements g and h of G, $g * h$ is an element of G;

(G1: associativity)
$(g * h) * k = g * (h * k)$ for all $g, h, k \in G$;

(G2: 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 $g \in G$;

(G3: 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:

(G4: commutativity) $g * h = h * g$ for all $g, h \in G$.

Addition modulo n

Given a natural number n, let
$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.
A binary operation $+_n$ (**addition modulo** n) on $\mathbb{Z}_n$ is defined for any $x, y \in \mathbb{Z}_n$ by

$$x +_n y = \begin{cases} x + y & \text{if } x + y < n, \\ x + y - n & \text{if } x + y \geq n. \end{cases}$$

Now let n be a positive real number and $\mathbb{R}_n = [0, n)$. The binary operation $+_n$ on $\mathbb{R}_n$ is defined by the same formula as above.

Theorem Each $(\mathbb{Z}_n, +_n)$ and each $(\mathbb{R}_n, +_n)$ is a group. All groups $(\mathbb{R}_n, +_n)$ are isomorphic.

Transformation groups

Definition. A **transformation group** is a group where elements are bijective transformations of a fixed set X and the operation is composition.

Examples.

- Symmetric group $S(X)$: all bijective functions $f : X \to X$.
- Translations of the real line: $T_c(x) = x + c$, $x \in \mathbb{R}$.
- $\mathrm{Homeo}(\mathbb{R})$: the group of all invertible functions $f : \mathbb{R} \to \mathbb{R}$ such that both f and f^{-1} are continuous (such functions are called **homeomorphisms**).
- $\mathrm{Homeo}^+(\mathbb{R})$: the group of all increasing functions in $\mathrm{Homeo}(\mathbb{R})$ (those that preserve orientation of the real line).
- $\mathrm{Diff}(\mathbb{R})$: the group of all invertible functions $f : \mathbb{R} \to \mathbb{R}$ such that both f and f^{-1} are continuously differentiable (such functions are called **diffeomorphisms**).

Matrix groups

A group is called **linear** if its elements are $n \times n$ matrices and the group operation is matrix multiplication.

- **General linear group** $GL(n, \mathbb{R})$ consists of all $n \times n$ matrices that are invertible (i.e., with nonzero determinant).

  The identity element is $I = \mathrm{diag}(1, 1, \ldots, 1)$.

- **Special linear group** $SL(n, \mathbb{R})$ consists of all $n \times n$ matrices with determinant 1.

  Closed under multiplication since $\det(AB) = \det(A) \det(B)$. Also, $\det(A^{-1}) = (\det(A))^{-1}$.

- **Orthogonal group** $O(n, \mathbb{R})$ consists of all orthogonal $n \times n$ matrices $(A^T = A^{-1})$.

- **Special orthogonal group** $SO(n, \mathbb{R})$ consists of all orthogonal $n \times n$ matrices with determinant 1.

  $SO(n, \mathbb{R}) = O(n, \mathbb{R}) \cap SL(n, \mathbb{R})$.

Semigroups

Definition. A **semigroup** is a binary structure $(S, *)$ that satisfies the following axioms:

(S0: closure)
for all elements g and h of S, $g * h$ is an element of S;

(S1: 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:

(S2: 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:

(S3: 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 $g, h_1, h_2 \in S$.

(S4: 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).
- 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 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 (strings) 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.

Basic properties of groups

- The identity element is unique.
- The inverse element is unique.
- $(g^{-1})^{-1} = g$. In other words, $h = g^{-1}$ if and only if $g = h^{-1}$.
- $(gh)^{-1} = h^{-1}g^{-1}$.
- $(g_1 g_2 \dots g_n)^{-1} = g_n^{-1} \dots g_2^{-1} g_1^{-1}$.
- Cancellation laws: $gh_1 = gh_2 \implies h_1 = h_2$ and $h_1 g = h_2 g \implies h_1 = h_2$ for all $g, h_1, h_2 \in G$.
- If $hg = g$ or $gh = g$ for some $g \in G$, then h is the identity element.
- $gh = e \iff hg = e \iff h = g^{-1}$.

Equations in groups

Theorem Let G be a group. For any $a, b, c \in G$,

- the equation $ax = b$ has a unique solution $x = a^{-1}b$;
- the equation $ya = b$ has a unique solution $y = ba^{-1}$;
- the equation $azc = b$ has a unique solution $z = a^{-1}bc^{-1}$.

Powers of an element

Let g be an element of a group G. The positive **powers** of g are defined inductively:

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

The negative powers of g are defined as the positive powers of its inverse: $g^{-k} = (g^{-1})^k$ for every positive integer k.
Finally, we set $g^0 = e$.

Theorem Let g be an element of a group G and $r, s \in \mathbb{Z}$. Then
(i) $g^r g^s = g^{r+s}$,
(ii) $(g^r)^s = g^{rs}$,
(iii) $(g^r)^{-1} = g^{-r}$.

Idea of the proof: First one proves the theorem for positive r, s by induction (induction on s for (i) and (ii), induction on r for (iii)). Then the general case is reduced to the case of positive r, s.

Order of an element

Let g be an element of a group G. We say that g has **finite order** if $g^n = e$ for some positive integer n.

If this is the case, then the smallest positive integer n with this property is called the **order** of g.

Otherwise g is said to be of **infinite order**.

Theorem If G is a finite group, then every element of G has finite order.

Proof: Let $g \in G$ and consider the list of powers: $g, g^2, g^3, \dots$. Since all elements in this list belong to the finite set G, there must be repetitions within the list. Assume that $g^r = g^s$ for some $0 < r < s$. Then $g^r e = g^r g^{s-r}$ $\implies g^{s-r} = e$ due to the cancellation law.

Subgroups

Definition. A group H is a called a **subgroup** of a group G if H is a subset of G and the group operation on H is obtained by restricting the group operation on G.

Proposition If H is a subgroup of G then **(i)** the identity element in H is the same as the identity element in G;
(ii) for any $g \in H$ the inverse g^{-1} taken in H is the same as the inverse taken in G.

Theorem Let H be a subset of a group G and define an operation on H by restricting the group operation of G. Then the following are equivalent:
(i) H is a subgroup of G;
(ii) H contains e and is closed under the operation and under taking the inverse, that is, $g, h \in H \implies gh \in H$ and $g \in H \implies g^{-1} \in H$;
(iii) H is nonempty and $g, h \in H \implies gh^{-1} \in H$.

Examples of subgroups: • $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.

• $(\mathbb{Q} \setminus \{0\}, \cdot)$ is a subgroup of $(\mathbb{R} \setminus \{0\}, \cdot)$.

• The special linear group $SL(n, \mathbb{R})$ is a subgroup of the general linear group $GL(n, \mathbb{R})$.

• The group of diffeomorphisms $\mathrm{Diff}(\mathbb{R})$ of the real line is a subgroup of the group $\mathrm{Homeo}(\mathbb{R})$ of homeomorphisms.

• Any group G is a subgroup of itself.

• If e is the identity element of a group G, then $\{e\}$ is the **trivial** subgroup of G.

Counterexamples: • $(\mathbb{R}^+, \cdot)$ is not a subgroup of $(\mathbb{R}, +)$ since the operations do not agree (even though the groups are isomorphic).

• $(\mathbb{Z}_n, +_n)$ is not a subgroup of $(\mathbb{Z}, +)$ since the operations do not agree (even though they do agree sometimes).

• $(\mathbb{Z} \setminus \{0\}, \cdot)$ is not a subgroup of $(\mathbb{R} \setminus \{0\}, \cdot)$ since $(\mathbb{Z} \setminus \{0\}, \cdot)$ is not a group (it is a **subsemigroup**).