Abstract Algebra, Lecture 3

Binary operations, semigroups, groups

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Summary

Summary

Definition

Let X be a set. A function

$$\star : X \times X \to X$$

is called a binary operation on X, or a rule of composition on X.

We often write $\star(x, y)$ in infix notation as $x \star y$.

Definition

The binary operation $\star$ on X is commutative if for all $x, y \in X$ it holds that

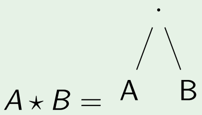
$$x \star y = y \star x$$

Definition

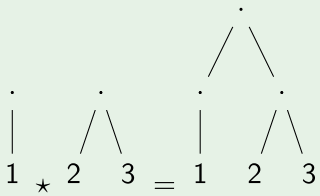
The binary operation $\star$ on X is associative if for all $x, y, z \in X$ it holds that
$$x \star (y \star z) = (x \star y) \star z$$
In this case, the resulting element can be unambiguously named $x \star y \star z$.

Example

X is the set of all rooted binary trees with at least one leaf, where the leaves are labeled by positive integers. If A, B are such trees, then

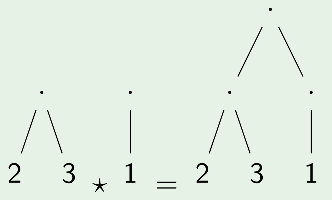


For example,



Example

On the other hand,



so the operation is not commutative. Neither is it associative.

Example

- X all 2x2-matrices (with real entries, say). $\star$ matrix multiplication. Associative product.
- X all invertible 2x2-matrices, with matrix multiplication. Associative product.
- X all 2x2-matrices, $A \star B = [A, B] = AB - BA$, commutator. $[B, A] = -[A, B]$, so not commutative (but skew-commutative.)
  Non-associative binary operation:

  $$[A, [B, C]] \neq [[A, B], C]$$

  in general.
  As an aside: "almost associative" by means of Jacobi triple identity:

  $$[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$$

Example

$M = \{a, b, c\}$, X all non-empty words on M, operation: concatenation.
Ex: $u = aaba, v = cbcaa$, $w = caba$

$$u * v = aabacbcaa \neq v * u = cbcaaaaba$$

$$u * (v * w) = aaba * (cbcaacaba) = aabacbcaacaba = (u * v) * w$$

This operation is associative, but not commutative.

Example

A set. X all maps $f : X \to X$. Operation: composition. This operation is associative, but not commutative.

Ex: $A = \{1, 2, 3\}$, $f(1) = 2$, $f(2) = 3$, $f(3) = 3$, $g(1) = 1$, $g(2) = 3$, $g(3) = 1$. $h = f \circ g$, $h(1) = f(g(1)) = f(1) = 2$, et cetera.

Definition

A set X with an associative binary operation is (by abuse of notation) called a semigroup. A semigroup is a monoid if there furthermore exists a (necessarily unique) identity element e such that

$$x \star e = e \star x = x$$

for all $x \in X$.

Example

- All "words" on an alphabet X form a semigroup under concatenation (the so-called free semigroup). Adjoin empty word to get free monoid.
- All "monomials" in X, e.g. if $X = a, b, c$ then elements $abaac = aaabc = a^3bc$, free commutative monoid.
- All 2x2-matrices under multiplication is a monoid.
- X^X, the set of all maps from X to itself, with composition as operation, is a monoid.

Example

$A = \{a, b\}$, $X = A^A$, operation composition. Then $X = \{I, S, P, Q\}$ with

$$I = \begin{pmatrix} a & b \\ a & b \end{pmatrix} \quad S = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$$
$$P = \begin{pmatrix} a & b \\ a & a \end{pmatrix} \quad Q = \begin{pmatrix} a & b \\ b & b \end{pmatrix}$$

Multiplication table

	I	S	P	Q
I	I	S	P	Q
S	S	I	Q	P
P	P	P	P	P
Q	Q	Q	Q	Q

Finally, the main object of study for the first part of the course:

Definition

A monoid $(X, \star, e)$ where each $x \in X$ has a (necessarily unique) two-sided inverse x^{-1}, i.e.,

$$x \star x^{-1} = x^{-1} \star x = e$$

is called a group.

Just to be difficult:

Definition

A group where the operation is commutative is called an Abelian group.

Example

All invertible maps $f : X \to X$ forms a group, the symmetric group S_X. Tremendously important and general.

Example

$X = \{1, 2, 3\}$. $f(1) = 2$, $f(2) = 1$, $f(3) = 3$, $g(1) = 2$, $g(2) = 3$, $g(3) = 1$. $(f \circ g)(1) = f(g(1)) = f(2) = 1$, $(g \circ f)(1) = g(f(1)) = g(2) = 3$, so $f \circ g \neq g \circ f$, so the group S_X is not abelian.

Example

- $(\mathbb{Z}, +, 0)$ is an abelian group.
- $(\mathbb{Q} \setminus \{0\}, *, 1)$ is an abelian group
- The set of invertible real $2x2$-matrices is a group
- The set of invertible linear transformation on a fixed vector space V is a group
- The set $\mathbb{Z}_n$ of integers mod n is a group under addition
- The set $U_n = \{ [k]_n | \gcd(k, n) = 1 \}$ is a group under multiplication

Henceforth, $(G, *, e)$ denotes a group.

Lemma

The inverse of $g \in G$ is unique.

Proof.

If h, k are inverses of g, then

$$h = h * e = h * (g * k) = (h * g) * k = e * k = e$$

$\square$

Lemma (Cancellation)

If $g, h, k \in H$ and $hg = kg$, then $h = k$.

Proof.

We have that $(hg)g^{-1} = (kg)g^{-1}$, thus $h(gg^{-1}) = k(gg^{-1})$, thus $h = k$. □

Lemma (Linear equations)

$a, b \in G$. The equation $ax = b$ has the unique solution $x = a^{-1}b$.

Proof.

Since $a * (a^{-1}b) = b$, this is one solution. If x is a solution, then $a^{-1}(ax) = a^{-1}b$. □

Example

Addition and multiplication modulo 5:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	0	1
2	2	3	0	1	2
3	3	0	1	2	3
4	4	1	2	3	4

$*$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$(\mathbb{Z}_5, +, [0])$ is an abelian group, as is U_5. Note that $ax = b$ (and $xa = b$) have a unique solution means that each element occurs exactly once in each row and in each column of the multiplication table.

Definition

Let $G = (G, *, e)$ be a group. A subset $H \subseteq G$ is a *subgroup*, denoted $G \leq H$, if

1. $e \in H$,
2. $a, b \in H \implies a * b \in H$,
3. $a \in H \implies a^{-1} \in H$.

Equivalently, $H \leq G$ if H, with the induced multiplication, forms a group.

Example

- $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$
- Let $\mathbb{C}^*$ denote the group of non-zero complex numbers, under multiplication.
  - The subset $\mathbb{R}^*$ of complex numbers with zero imaginary part is a subgroup,
  - The set $i\mathbb{R}^*$ of complex numbers with zero real part is *not* a subgroup,
  - The subset of complex numbers with unit modulus is a subgrup, the so-called circle group $\mathfrak{T}$
  - The subset of complex numbers with modulus 2 is not a subgroup,
  - The subset of complex numbers with rational real and imaginary parts forms a subgroup,
  - The subset of complex with with rational real and imaginary parts, and unit modulus, forms a subgroup. Elements of this infinite subgroup correspond to Pythagorean Triplets.
- The set of all invertible linear transformations on a real vector space V is a subgroup of the group S_V of all invertible maps from V to itself.

Lemma

If $H \leq K \leq G$ then $H \leq G$.

Lemma

If $H \leq G$ and $K \leq G$ then $H \cap K \leq G$.

Lemma

If $S \subseteq G$ is any subset, then the intersection of all subgroups of G that contains S is a subgroup, denoted by $\langle S \rangle$. This is the unique smallest subgroup that contains S.