KTH Teknikvetenskap

SF2729 GROUPS AND RINGS
LECTURE NOTES
2010-01-27

MATS BOIJ

1. THE FIRST LECTURE - BINARY OPERATIONS AND GROUPS

The first lecture in the course presents some basic ideas of algebra and introduces the notions of binary operations and groups.[1]

Definition 1.1 (Binary operation)**.** A *binary operation* on a set, S, is a rule which to every pair of elements in S assigns an element S. We can view this as a function

$$S \times S \longrightarrow S$$

and we usually write this as $a * b = c$ if the pair (a, b) is sent to c. However, the symbol $*$ may vary.

Example 1.1. Here are some well-known examples of binary operations:

(1) The integers $\mathbb{Z}$ has three natural binary operations, $+$ (addtion), $-$ (subtraction) and $\cdot$ (multiplication).
(2) On $\mathbb{R}^3$, the vector product $\times$ defines a binary operator.
(3) On the set of $n \times n$-matrices, matrix multiplication defines a binary operation.
(4) On the set of functions $f : X \longrightarrow X$ on any set X, composition $\circ$ defines a binary operation.

In many such instances, but not all, we will be able to use the operation on several elements in a row to get $a * b * c$. In order for this to work, we need that

$$(a * b) * c = a * (b * c),$$

for all a, b och c i S. In this case, we say that the operation is *associative*. Our usual addition and multiplication are examples of such operations as well as compositions of functions.

An element e satisfying $a * e = a * e = a$ for all elements in S is called *neutral*, *unit* eller *identity element*.

[1]The first lecture is based on the sections1-4 of Chapter I in A First Course in Abstract Algebra [1].

If there is a unit we may say that a certain element a is *invertible* if there is an element b such that

$$a * b = b * a = e.$$

If we have that $a * b = b * a$ for all elements a and b, we say that the operation is *commutative*.

Definition 1.2. Two binary structures on two sets S and T are said to be *isomorphic* if there is a bijective function $f : S \longrightarrow T$ such that

$$S(a * b) = S(a) *' S(b)$$

for all $a, b \in S$, where $*$ is the binary operation on S and $*'$ is the binary operation on T.

If the binary structures are isomorphic we cannot distinguish them after changing the names of the elements according to the bijection preserving the binary operation.

Example 1.2. The binary structures given by $+$ on the real numbers $\mathbb{R}$ by $\cdot$ on the positive real numbers are isomorphic since

$$\exp : \mathbb{R} \longrightarrow \mathbb{R}^+$$

is a bijection satisfying

$$\exp(a + b) = \exp(a) \cdot \exp(b)$$

for all $a, b \in \mathbb{R}$. (Observe that the same is not true for $\exp : \mathbb{C} \longrightarrow \mathbb{C}^*$.)

Exercise 1.1. *Show that $[A, B] = AB - BA$ defines a binary operation on the set of real skew-symmetric $n \times n$-matrices. Futhermore, show that for $n = 3$, this binary structure is isomorphic to the binary structure given by the vector product on $\mathbb{R}^3$.*

Definition 1.3 (Group)**.** A *group* is a set G with a binary operation $*$ satisfying

(1) $*$ is associative, i.e., $a * (b * c) = (a * b) * c$, for all $a, b, c \in G$.
(2) G has a unit, i.e., an element e such that $a * e = e * a = a$ for all $a \in G$.
(3) Every element in G is invertible, i.e., for all $a \in G$ we can find $b \in G$ such that $a * b = b * a = e$.

Definition 1.4 (Abelian group)**.** If the group operation is *commutative*, i.e., if

$$a * b = b * a$$

for all a and b, we say that the group is *abelian*. In this case, the group operation is often written as $+$ and the unit as 0.

Example 1.3. All the kinds of numbers that we have seen so far form abelian groups with respect to addition, e.g., integers $\mathbb{Z}$, rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$.

Example 1.4. On any set X, the set S_X of bijective functions $\sigma : X \longrightarrow X$ forms a group under composition, $\circ$. When $X = \{1, 2, \ldots, n\}$ we usually denote this group by S_n - the *symmetric group* on n elements. In general S_X is the *symmetric group on X*.

Example 1.5. The set of invertible real $n \times n$-matrices forms a group under matrix multiplication, the *general linear group*, $\mathrm{Gl}_n(\mathbb{R})$.

Example 1.6. The set of symmetries of a given geoemtric object forms a group under composition. A *symmety* of an object is a solid body motion that makes the object look the same before and after.

Example 1.7 (The dihedral group, D_{2n}, the symmetries of an n-gon)**.** If we look at the symmetris of a regular n-gon in the plane, we get a group D_{2n} with $2n$ different elements, of which n are rotations and n are reflections.

Using the standard basis for the plane $\mathbb{R}^2$, we can write down the matrices fot these symmetries as

$$r_j = \begin{pmatrix} \cos\left(\frac{2\pi j}{n}\right) & -\sin\left(\frac{2\pi j}{n}\right) \\ \sin\left(\frac{2\pi j}{n}\right) & \cos\left(\frac{2\pi j}{n}\right) \end{pmatrix} \quad \text{och} \quad s_j = \begin{pmatrix} \sin\left(\frac{2\pi j}{n}\right) & \cos\left(\frac{2\pi j}{n}\right) \\ \cos\left(\frac{2\pi j}{n}\right) & -\sin\left(\frac{2\pi j}{n}\right) \end{pmatrix}$$

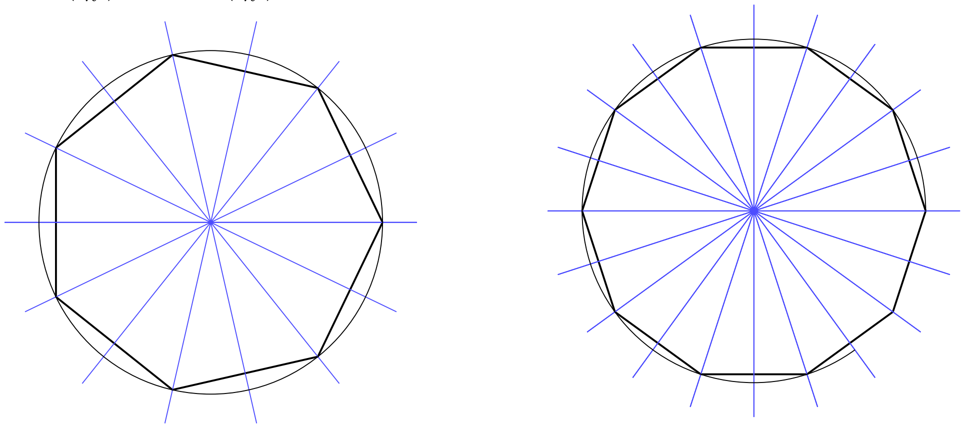
We may now use the addition laws for sine and cosine to verify that the products of these matrices are given by

$$r_j r_k = r_{j+k}, \quad r_j s_k = s_{k-j}, \quad s_j r_k = s_{j+k}, \quad s_j s_k = r_{k-j},$$

We may also pass to the complex numbers and change bases in $\mathbb{C}^2$. We get

$$r_j = \begin{pmatrix} \xi^j & 0 \\ 0 & \xi^{-j} \end{pmatrix} \quad \text{och} \quad s_j = \begin{pmatrix} 0 & \xi^{-j} \\ \xi^j & 0 \end{pmatrix}$$

where $\xi = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$. is a primitive root of unity.



RECOMMENDED EXCERCISES

I-1 Introduction and Examples. 35-37

I-2 Binary Operations. 24, 26, 29-34

I-3 Isomorphic Binary Structures. 26, 27, 28

I-4 Groups. 11-18, 23, 25, 29, 32, 33, 35, 37, 38

REFERENCES

[1] J. B. Fraleigh. *A First Course In Abstract Algebra*. Addison Wesley, seventh edition, 2003.