Algebraic Structures

University of Ostrava

Version of May 5, 2021

Literature

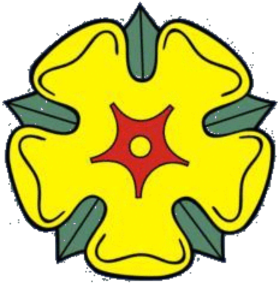
- S. Lang, *Algebra*, revised 3rd ed., Springer, 2002
(referred in what follows as LANG)
- S. Mac Lane and G. Birkhoff, *Algebra*, 3rd ed., AMS Chelsea, 1999
(referred as MAC LANE–BIRKHOFF)
- I.R. Shafarevich, Basic Notions of Algebra, Springer, 1990
(referred as SHAFAREVICH)

(All images are courtesy of Wikipedia)

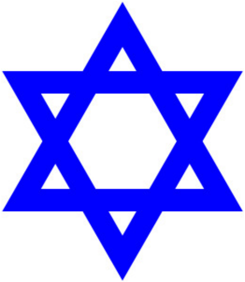
Groups

Groups

The notion of group embodies the idea of symmetry and is one of the central notions in mathematics.



$\mathbb{Z}/5\mathbb{Z}$



$\mathbb{D}_6$

Algebraic structures

From the linear algebra course(s) you know the definition of vector space: this is a set subject to given operations (addition, multiplication on scalars) satisfying given axioms (commutativity, associativity, existing of zero, etc.)

This is an instance of an *algebraic structure*: $\langle X, f_1, f_2, \dots \rangle$; the set X with a number of (generally, multiary) operations $f_i : X \times \cdots \times X \to X$, satisfying certain axioms.

Groups (and other things we will study in due course, like rings and fields) is another instance of algebraic structures.

Groups (cont.)

Definition

A *group* is a set G with a binary operation $\cdot : G \times G \to G$ (called *multiplication*), and a distinguished element $e \in G$ (called the *unit*, or the *neutral element*) subject to the following axioms:

- For any $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associativity).
- For any $a \in G$, $a \cdot e = e \cdot a = a$.
- For any $a \in G$ there exists an element $a^{-1} \in G$ (called the *inverse* of a) such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

The cardinality of the set G is called an *order* of the group.

Examples of groups

- The *trivial* group consisting of one element e.
- All symmetries of a geometric figure (i.e., continuous transformations mapping the figure to itself) subject to operation of composition from the first slide.
- All permutations of a finite set of n elements, called the *symmetric group* S_n.
- All invertible transformations of a vector space V subject to operation of composition, called the *general linear group* $GL(V)$.
- $(\mathbb{Q}, +)$, $(\mathbb{Q}\backslash\{0\}, \times)$.

Exercise 1

What are the orders of these groups?

Exercise 2

Can you give more examples? What is a general pattern for constructing them?

See also Shafarevich, pp. 105,109–118,144-150.

Multiplication table

Group can be given by enumerating elements, and specifying explicitly the table of all products between them (called the *multiplication table*).

Groups of order 2 and 3:

	e	a
e	e	a
a	a	e

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Exercise

Are there other groups of orders 2 and 3?

For a list of small groups, see SHAFAREVICH, p. 152.

Another exercise

What is the minimal number *n* such that if one removes *n* rows and *n* columns from the multiplication table of an arbitrary finite group, it is always possible to reconstruct the group from the incomplete table?

(Proposed to, and, unfortunately, got rejected at the 2017 Vojtěch Jarník International Mathematical Competition)

Subgroups

Generally, a *substructure* of an algebraic structure $\langle X, f_1, f_2, \dots \rangle$ is a subset of X closed with respect to all operations $f_1, f_2, \dots$.

Accordingly:

Definition

A *subgroup* of a group G is a subset closed with respect to multiplication, and taking the inverse (and hence containing the unit).

(Note that distinguished elements of an algebraic structure, if any, can be interpreted as 0-ary operations, thus any substructure should contain them).

Homomorphisms and automorphisms

Generally, a *homomorphism* between two algebraic structures $\langle X, f_1, f_2, \dots \rangle$ and $\langle Y, f_1, f_2, \dots \rangle$ of the same signature (i.e., having the same number of operations of the same arity) is a map $X \to Y$ which preserves any of the operations $f_1, f_2, \dots$. A homomorphism is called an *isomorphism* (and X and Y are said *isomorphic*, notationally $X \simeq Y$), if it is bijective. An isomorphism of an algebraic structure to itself is called *automorphism*.

Automorphisms of any algebraic structure X form a group with respect to composition, denoted by $Aut(X)$. This is one of the reasons groups occupy a central place among all possible algebraic structures.

Homomorphisms of groups

According to the general notion from the previous slide:

Definition

A *homomorphism* from a group G to a group H is a map $f : G \to H$ such that $f(a \cdot b) = f(a) \cdot f(b)$ for any $a, b \in G$, and $f(e) = e$ (note that, by abuse of notation, the multiplication and unit in the groups G, H are denoted by the same symbols).

Exercise

Prove that if f is a homomorphism of groups, then $f(a^{-1}) = f(a)^{-1}$.

Examples of group homomorphisms

- For any $a \in G$, $x \mapsto a^{-1}xa$ is an automorphism of a group G, called an *inner automorphism*.
- $det : GL_n(K) \to K^*$
- $log : (\mathbb{R}_{>0}, \times) \to (\mathbb{R}, +)$

Normal subgroups

Definition

The *kernel* of a group homomorphism $f : G \to H$ is the set $\{a \in G \mid f(a) = e\}$.

Definition

A subgroup N of a group G is called *normal subgroup* (denoted as $N \triangleleft G$), if $a^{-1}xa \in N$ for any $x \in N$ and $a \in G$.

In other words: N is stable under all inner automorphisms.

Yet in other words: any *left coset* is also a *right coset*: $aN = Na$ for any $a \in G$.

In any group G, the trivial subgroup, $\{e\}$, and the whole group G, are normal subgroups.

Definition

All normal subgroups besides $\{e\}$ and G are called *proper*.

Normal subgroups and quotients

Theorem

Normal subgroups are precisely kernels of group homomorphisms.

(That is, the kernel of any group homomorphism is a normal subgroup, and any normal subgroup is the kernel of a suitable group homomorphism).

For a given normal subgroup N of a group G, the homomorphism from the theorem is constructed as follows. Define an equivalence relation on G: $a \sim b$ if $aN = bN$. (Prove that this is an equivalence relation!). On the set of equivalence classes – the cosets – define multiplication as:

$$(aN) \cdot (bN) = abN.$$

(Why this is well defined?). Thus obtained structure is a group, denoted as G/N, and called the *group of quotients* of G by N.

Examples of normal subgroups and group quotients

- $n\mathbb{Z} \triangleleft \mathbb{Z}$ for any integer n.
- $GL_n(K)/\{\text{scalar matrices}\} \simeq SL_n(K)$, the group of $n \times n$ matrices with determinant 1.

For more examples, see SHAFAREVICH, pp. 107,141 and LANG, p. 15.

Homomorphism theorems, 1 and 2

The first homomorphism theorem

If $f : G \to H$ is a group homomorphism, then there is a group isomorphism $G/Ker\, f \simeq Im\, f$.

The second homomorphism theorem

If H is a normal subgroup in a group G, K a normal subgroup both in H and in G, then H/K is a normal subgroup in G/K, and

$$(G/K)/(H/K) \simeq G/H.$$

Warning

The relation of normality in groups is not transitive! That is, if $K \triangleleft H \triangleleft G$, then not necessarily $K \triangleleft G$. (Give an example!).

Homomorphism theorem, 3

The third homomorphism theorem

If S is a subgroup in a group G, and N a normal subgroup in G, then $N \cap S$ is a normal subgroup in S, NS is a subgroup in G, and

$$S/(N \cap S) \simeq NS/N.$$

These three homomorphism theorems are valid in a much more general context, for general algebraic systems.

Direct product of groups

Definition

A *direct product* of two groups G, H is the group formed by the Cartesian product $G \times H$ with respect to multiplication defined as

$$(a, b) \cdot (a', b') = (aa', bb')$$

for any $a, a' \in G$, $h, h' \in H$.

Lemma

$G \times \{e\}$ is a normal subgroup in $G \times H$, and $(G \times H)/(G \times \{e\}) \simeq H$. (Similarly for $\{e\} \times H$).

Cyclic groups

Definition

A group G is *cyclic*, if there is an element $a \in G$ such that every element of G is of the form a^n for some integer n.

Theorem

Any infinite cyclic group is isomorphic to $\mathbb{Z}$. Any finite cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Commutator and commutant

Definition

A *commutator* of two elements a, b of a group G is defined as $a^{-1}b^{-1}ab$. A *commutant* of a group G, denoted by $[G, G]$, is a subgroup generated by all commutators.

Abelian groups

Definition

A group G is called *commutative*, or *abelian*, if the multiplication is commutative: $a \cdot b = b \cdot a$ for any $a, b \in G$.

In other words, the commutator of G is trivial: $[G, G] = \{e\}$.

"Abelian" is in honor of Niels Henrik Abel (1802–1829):

Exercise

Which of the groups considered so far are abelian?

Nilpotent groups

Definition

A *lower central series* G^n of a group G is defined inductively as: $G^1 = G$, $G^{n+1} = [G^n, G]$. A group G is called *nilpotent*, if $G^n = 0$ for some n.

Example

The group of all upper-triangular $n \times n$ matrices over a field with units on the diagonal.

Solvable groups

Definition

A *derived series* $G^{(n)}$ of a group G is defined inductively as: $G^{(1)} = G$, $G^{(n+1)} = [G^{(n)}, G^{(n)}]$. A group G is called *solvable*, if $G^{(n)} = 0$ for some n.

The term "solvable" comes from Galois theory – named after Évariste Galois (1811–1832) – which links properties of an algebraic equation with the group of its symmetries: an algebraic equation is solvable in radicals if and only if the group of all permutations of its roots is solvable.

Nilpotent and solvable groups

Lemma

Any nilpotent group is solvable.

Example of solvable groups

- S_3, S_4.
- The group of all upper-triangular $n \times n$ matrices over a field.

For more examples, see Shafarevich, p. 156.

Theorem

A subgroup and a homomorphic image of a cyclic, respectively abelian, respectively nilpotent, respectively solvable group, is cyclic, respectively abelian, respectively nilpotent, respectively solvable. A direct product of abelian, respectively nilpotent, respectively solvable groups, is abelian, respectively nilpotent, respectively solvable.

Simple groups

Definition

A group is called *simple* if all its normal subgroups are proper.

Theorem

An abelian group is simple if and only if it is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Another example

The *alternating group* A_n consisting of even permutations in S_n, for $n \geq 5$.

For more examples, see Shafarevich, p. 157–160.

Rings

Rings

Definition

A *ring* is a set R with two binary operations $+, \cdot : R \times R \to R$ (called *addition* and *multiplication* respectively) and distinguished element 0 (called *zero*), subject to the following axioms:

- R is an abelian group with respect to addition and with 0 as a neutral element.
- For any $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associativity of multiplication).
- For any $a \in R$, $a \cdot 0 = 0 \cdot a = 0$.
- For any $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ (distributivity).

Exercise

Give definitions: of a subring of a ring; of a homomorphism and isomorphism of rings.

Examples of rings

- Integers $\mathbb{Z}$.
- $GF(2)$, the ring consisting of two elements $\{0, 1\}$, where $1 \cdot 1 = 1$

Exercise

Are there other (nonisomorphic!) rings consisting of two elements?

- Polynomial ring $K[x]$: all polynomials with coefficients in a field K.
- Matrix ring $M_n(K)$ of all $n \times n$ matrices with coefficients in K.
- The set of continuous real-valued functions defined on the same topological space.

Definition

A ring R is called *commutative*, if $a \cdot b = b \cdot a$ for any $a, b \in R$.

Exercise

Give more examples. Which of all these rings are commutative? Give examples of subrings in all these rings.

Examples of homomorphisms of rings

- $\mathbb{Z} \to GF(2)$: even number $\mapsto 0$, odd number $\mapsto 1$.
- Evaluation homomorphism: from the ring of real functions to $\mathbb{R}$: $f \mapsto f(x_0)$ for some fixed x_0 in the domain.

Ideals

The following goes very similarly with the group case.

Definition

The *kernel* of a ring homomorphism $f : R \to S$ is the set $\{a \in R \mid f(a) = 0\}$.

Definition

An subring I of a ring R is called an *ideal*, if $x \cdot a \in I$ and $a \cdot x \in I$ for any $x \in I$, $a \in R$.

In any ring R, $\{0\}$ (denoted by abuse of notation just as 0), and the whole R are always ideals.

Definition

All ideals besides 0 and R are called *proper ideals*.

Theorem

Ideals are precisely kernels of homomorphisms.

Quotients

Let I be an ideal of a ring R. Define an equivalence relation on R: $a \sim b$ if $a - b \in I$. On the set of equivalence classes define addition and multiplication as:

$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I) \cdot (b + I) = ab + I.$$

Thus obtained structure is a ring, denoted as R/I, and called the *ring of quotients* of R by I.

The three homomorphism theorems similar to those for groups, are valid for rings.

Direct sums

Definition

A *direct sum* of two rings R and S, denoted by $R \oplus S$, is the ring consisting of all pairs from $R \times S$ (cartesian product) with addition an multiplication defined component-wise:

$$(r, s) + (r', s') = (r + r', s + s')$$
$$(r, s) \cdot (r', s') = (r \cdot r', s \cdot s')$$

for any $r, r' \in R$, $s, s' \in S$.

Exercise

Establish a ring isomorphism $R \oplus S \simeq S \oplus R$.

Fields

Fields

Definition

A *field* is a set F with two binary operations $+, \cdot : F \times F \to F$ (called *addition* and *multiplication* respectively) and two distinguished elements 0 and 1 (called the *zero* and the *unit* respectively), subject to the following axioms:

- F is a commutative ring with respect to addition and multiplication.
- For any $a \in F$, $a \cdot 1 = a$.
- For any $a \in F$, there is an element $a^{-1} \in F$ (called the *inverse* of a), such that $a \cdot a^{-1} = 1$.

Fields (cont.)

In other words, F is an abelian group with respect to addition (called the *additive group* of F), and $F^* = F \backslash \{0\}$ is an abelian group with respect to multiplication (called the *multiplicative group* of F).

Yet in other words, F is a commutative ring with unit all whose nonzero elements are invertible.

Exercise

Give definitions: of a subfield of a field; of an isomorphism of fields. Why we do not speak about homomorphism of fields?

Theorem

A commutative ring with unit is a field if and only if it does not have any proper ideals.

Examples

Examples of fields

- Number fields: rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, complex numbers $\mathbb{C}$. We have a chain of subfields: $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
- $GF(2)$ is actually a field, the smallest possible one.
- The polynomial ring $K[x]$ is not a field. (Prove this!). But if we consider $K(x)$, the set of all formal "fractions" with elements from $K[x]$, i.e., all expressions of the form $\frac{f(x)}{g(x)}$, where $f(x), g(x) \in K[x]$, with the usual rules for addition and multiplication of fractions, then it becomes a field. (Prove this!)

Example of a field isomorphism

$\mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$

Algebraically closed fields

Definition

A field F is called *algebraically closed*, if every polynomial with coefficients in F has a root in F

Examples

$\mathbb{C}$ is algebraically closed, while $\mathbb{R}$ or finite fields are not.

Theorem

Any field has an algebraically closed extension.

Definition

Given a field F, such minimal extension is called an *algebraic closure* of F, and is denoted by $\overline{F}$.

Example

$\overline{\mathbb{R}} = \mathbb{C}$

Characteristic

Definition

A *characteristic* of a field is the minimal number n such that $\underbrace{1 + \cdots + 1}_{n \text{ times}} = 0$, or zero if such number does not exist.

Theorem

A characteristic of a field is either 0, or a prime number.

Examples

Characteristic of $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ is zero, characteristic of $GF(2)$ is 2.

Finite fields

We have already encountered a finite field of 2 elements, $GF(2)$.

Theorem 1

The ring quotient $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.

This field is denoted by $GF(p)$.

Theorem 2

1. The number of elements of a finite field has the form p^n, where p is the characteristic of the field;
2. For each prime p and positive integer n there exists a field of p^n elements;
3. Two finite fields with the same number of elements are isomorphic.

The unique, according to this theorem, field of p^n elements is denoted by $GF(p^n)$. ("GF" stands for "Galois field").

Exercise

Draw multiplication tables for the field $GF(4)$.

Prime subfields

Theorem

Every field F contains a minimal subfield P (i.e., any other subfield of F contains P), which is isomorphic either to $\mathbb{Q}$ (if characteristic of F is zero), or to $GF(p)$ (of characteristic of F is p).

Definition

This subfield P is called a *prime subfield* of F.

Algebras

Algebras

Algebra = ring + vector space.

Definition

An *algebra* over a field K is a vector space A over a field K with a binary operation $\cdot : A \times A \to A$ such that $(A, +, \cdot)$ is a ring, and additionally, the following axiom is satisfied: $\lambda(a \cdot b) = (\lambda a) \cdot b$ for any $a, b \in A$, $\lambda \in K$.

Terminological warning

"Algebra" has (at least) two (related) meanings: first, a part of mathematics, and second, a particular mathematical structure (which is studied in the scope of algebra in the first sense).

Example of algebras

- The polynomial ring $K[x]$, and the matrix ring $M_n(K)$ are, actually, algebras over the field K.
- Power series $K[[x]]$ over a field K.

Structure constants

If we fix a basis $\{e_i\}_{i \in I}$ in an algebra A, then the multiplication in A is uniquely determined by multiplication between all pairs of the elements of the basis ("multiplication table"):

$$e_i \cdot e_j = \sum_{i \in I} C_{ij}^k e_k,$$

where $i, j \in I$. The elements of the base field $\{C_{ij}^k\}_{i,j,k \in I}$ are called *structure constants* of A in the basis $\{e_i\}$.

Example

The matrix units E_{ij}, $i, j = 1, \dots, n$ form a basis of the matrix algebra $M_n(K)$. The multiplication table in this basis is

$$E_{ij} E_{k\ell} = \delta_{jk} E_{i\ell}.$$

Exercise

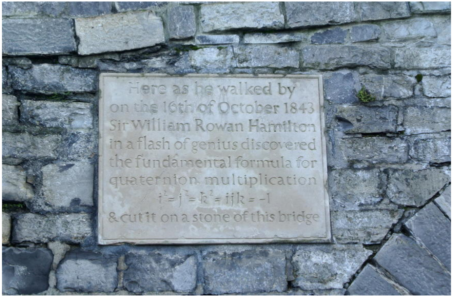
Take a few low-dimensional algebras and write their structure constants in some bases.

Quaternions

Definition

The *quaternion algebra* $\mathbb{H}$ over a field K is the 4-dimensional algebra with the basis $\{1, i, j, k\}$, where 1 is the unit, and the rest of multiplication table is

$i^2 = j^2 = k^2 = -1, ij = k, ji = -k, jk = i, kj = -i, ki = j, ik = -j$


Here as he walked by
on the 16th of October 1843
Sir William Rowan Hamilton
in a flash of genius discovered
the fundamental formula for
quaternion multiplication
$i^2 = j^2 = k^2 = ijk = -1$
& cut it on a stone of this bridge

For more about quaternions and why they are important, see Shafarevich, pp. 65–66 and Mac Lane–Birkhoff, pp. 281–283.

Modules

Modules

Modules is a generalization of the concept of vector space, where instead of the underlying field we are taking a ring: the axioms are exactly the same as for the vector space, with multiplication by elements of a field being replaced by multiplication by element of a ring.

Examples

- A ring is a module over itself.
- More generally, an ideal in a ring is module over that ring.
- The vector space of vector fields (say, in the 2-dimensional real space) $\{f(x,y)\partial/\partial x + g(x,y)\partial/\partial y\}$ is a module over a ring of functions.
- Abelian groups are nothing but modules over $\mathbb{Z}$.

For more examples see Shafarevich, pp. 34–36.

Modules (cont.)

Exercise

Give definitions of a submodule, a homomorphism of modules, and a quotient module.

Tensor product

The tensor product is an analog of “multiplication” for modules.

Theorem

Let M, N be two modules over a ring R. Consider a class of modules L such that there is a “multiplication” map $M \times N \to L$, $(x, y) \mapsto xy$ satisfying the following bilinearity properties:

$$(x_1 + x_2)y = x_1y + x_2y \text{ for any } x_1, x_2 \in M, y \in N$$
$$x(y_1 + y_2) = xy_1 + xy_2 \text{ for any } x \in M, y_1, y_2 \in M$$
$$(ax)y = x(ay) = a(xy) \text{ for any } a \in R, x \in M, y \in N.$$

Then there is a “universal” module in this class, denoted by $M \otimes_R N$ with multiplication denoted by $x \otimes y$: for any other module L in the class, there exists a unique homomorphism $\varphi : M \otimes_R N \to L$ such that $xy = \varphi(x \otimes y)$.

Definition

The module $M \otimes_R N$ is called the *tensor product* of the modules M and N.

Tensor product (cont.)

The tensor product $M \otimes_R N$ can be constructed explicitly as a submodule of the R-module generated by $M \times N$ subject to the following relations:

$$
\begin{gathered}
(x_1 + x_2, y) - (x_1, y) - (x_2, y) \\
(x, y_1 + y_2) - (x, y_1) - (x, y_2) \\
a(x, y) - (x, ay) \\
a(x, y) - (ax, y).
\end{gathered}
$$

Theorem

If R is a field (i.e., M and N are vector spaces over R, and $\{e_i\}_{i \in I}$ and $\{f_i\}_{i \in J}$ are R-bases of M and N respectively, then $\{e_i \otimes f_j\}_{i \in I, j \in J}$ is a basis of the R-vector space $M \otimes_R N$.

Corollary

If R is a field, then $\dim(M \otimes_R N) = \dim M \cdot \dim N$.

Tensor product (cont.)

Warning

The intuition for the tensor product of vector spaces works badly in the general case. For example, if n and m are relatively prime, then $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} = 0$. (Prove this!)

We can go further and iterate the tensor product construction. In particular, tensoring the same module M with itself, and taking direct sums of all tensor powers, we get the *tensor algebra* of M, and taking in it various quotients and subspaces we get symmetric and skew-symmetric powers, etc. See Shafarevich, pp. 38–39, Lang, pp. 601–612, 632–637, and Mac Lane–Birkhoff, pp. 522–547 for details.

The End