additive

A function \( f : G \rightarrow H \) from a semigroup \( G \) to a semigroup \( H \) is [additive] if \( f(a + b) = f(a) + f(b) \). A group-valued function on sets is additive if \( f(Y \cup Z) = f(Y) + f(Z) \) if \( Y \) and \( Z \) are disjoint.

algebra

An [algebra] over a field \( K \) is a ring with 1 which is also a vector space over \( K \) and whose multiplication is bilinear with respect to \( K \). Examples:

- the complex numbers \( C \) is an algebra over the field of real numbers \( K = R \).
- The quaternion algebra \( H \) is an algebra over the field of complex numbers.
- The matrix algebra \( M(n, R) \) is an algebra over the field \( R \).

An algebraic number field

[An algebraic number field] is a subfield of the complex numbers that arises as a finite degree algebraic extension field over the field of rationals.

alternating group

The [alternating group] \( G \) is the subgroup of the symmetric group of \( n \) objects given by the elements which can be written as a product of an even number of transpositions.

Artinian module

An [Artinian module] is a module which satisfies the descending chain condition. Every Artinian module is a Noetherian module but the integers for example are a Noetherian module which is not an Artinian module.

Artinian ring

An [Artinian ring] is a ring which when considered as a \( R \)-module is an Artinian module.

Artinian ring

Two elements of an integral domain that are unit-multipliers of each other are called [associate numbers].
Cayley’s theorem

[Cayley’s theorem] assures that every finite group is isomorphic to a permutation group.

center

The [center] of a group \((G, \ast)\) is the set of all elements \(g\) which satisfy \(gh = hg\) for all \(h\) in \(G\). The center is a subgroup of \(G\).

commutator

The [commutator] of two elements \(g, h\) in a group \((G, \ast)\) is defined as \([g, h] = g \ast h \ast g^{-1} \ast h^{-1}\).

commutator subgroup

The [commutator subgroup] of a group \((G, \ast)\) is the set of all commutators \([g, h]\) in \(G\). It is a subgroup of \(G\).

factor group

A [factor group] \(G/N\) is defined when \(N\) is a normal subgroup of the group \(G\). It is the group, where the elements are equivalent classes \(gN\) and operation \((gN)(hN) = (gh)N\) which is defined because \(N\) was assumed to be normal. For example, if \(G\) is the group of additive integers and \(N = kN\) with an integer \(k\), then \(G/N = Z_k\) is finite group of integers modulo \(k\).

finite group

A group is called a [finite group] if \(G\) is a set with finitely many elements. For example, the set of all permutations of a finite set form a finite group. The set of all operations on the Rubik cube form a finite group.
A [group] \((X, +, 0)\) is a set \(X\) with a binary operation \(+\) and a zero element \(0\) (also called neutral element or identity) with the following properties

\[
(a + b) + c = a + (b + c) \quad \text{associativity}
\]
\[
a + 0 = a \quad \text{zero element}
\]
\[
\forall a \exists b a + b = 0 \quad \text{inverse}
\]

Examples:

- the real numbers form a group under addition \(5 + 2.34 = 7.34, 3 - 3 = 0\).
- the set \(GL(n, R)\) of real matrices with nonzero determinant form a group under matrix multiplication
- the nonzero integers form a group under multiplication \(4 \times 7 = 28\).
- all the invertible linear transformations of the plane form a group under composition. The "zero element" is the identity transformation \(T(x) = x\).
- all the continuous functions on the unit interval form a group with addition \((f + g)(x) = f(x) + g(x)\).
- all the permutations on a finite set form a group under composition.
- the set of subsets \(Y\) of a set \(X\) with the operation \(A \Delta B = (A \cup B) \setminus (A \cap B)\) form a group. The inverse of \(A\) is \(A\) itself because \(A \Delta A = \emptyset\), the zero element is \(\emptyset\).

A [normal subgroup] of a group \((G, \ast)\) is a subgroup \((H, \ast)\) of \((G, \ast)\) which has the property that for all \(g\) in \(H\) and all \(g\) in \(G\) one has \(g^{-1}hg\) is in \(H\). For an abelian group all subgroups are normal. The subgroup \(Sl(n, R)\) of \(Gl(n, R)\) is a normal subgroup.

A [ring] \((X, +, \ast, 0)\) is a set \(X\) with a binary operation \(+\) and a binary operation \(\ast\) such that \((X, +, 0)\) is a commutative group and \((X, \ast)\) is a semigroup and such that the distributivity laws \(a \ast (b + c) = a \ast b + a \ast c\), \((a + b) \ast c = a \ast c + b \ast c\) hold. Examples:

- the integers \(Z\) form a ring with addition and multiplication
- the set of rational numbers \(Q\), the set of real numbers \(R\) or the complex numbers \(C\) form a ring with addition and multiplication.
- the set of 3x3 matrices with real entries form a ring with addition and matrix multiplication.
- the set \(P\) of polynomials with real coefficients form a ring with addition and multiplication.
- the set of subsets \(Y\) of a set \(X\) with addition \(\Delta\) and multiplication \(\cap\) forms a ring.
- the set of continuous functions on an interval \([0, 1]\) with addition \((f + g)(x) = f(x) + g(x)\) and multiplication \(f \ast g(x) = f(x)g(x)\).
A [commutative group] is a group \((X, +, 0)\) which is commutative: \(a + b = b + a\).

- the set of real numbers \(R\) forms a commutative group under addition.
- the set of permutations \(S\) of a set \(X\) form a noncommutative group under composition.

A [commutative ring] is a ring \((X, +, *, 0)\) for which the multiplicative semigroup \((X, *)\) is commutative: \(a * b = b * a\). Examples:

- the integers form a commutative ring.
- the set of \(2 \times 2\) matrices form a noncommutative ring
- the set of polynomials with real coefficients \((x^2 + \pi x + 2) * (x + 5x) = 6x^3 + 6\pi x^2 + 12x\).

A [function field] is a finite extension of the field \(C(z)\) of rational functions in the variable \(z\).

An [homomorphism] \(\phi\) between two groups \(G, H\) is a map \(f : G \to H\) which has the property \(\phi(g * h) = \phi(g) * \phi(h)\) and \(\phi(0) = 0\) for all elements \(g, h \in G\). Examples:

- if \(G\) is the multiplicative group \((R^+, *)\) of positive real numbers and \(H\) is the additive group \((R, +)\) of all positive real numbers then \(\phi(x) = \log(x)\) is a homomorphism:
- if \(G\) is the group of matrices with nonzero determinant and \(H\) is the group of nonzero real numbers and \(\phi(A) = \det(A)\), we have \(\phi(x * y) = \phi(x)\phi(y)\).

An [isomorphism] \(\phi\) between two groups \(G, H\) is a homomorphism between groups which is also invertible.
A number field is a finite extension of $\mathbb{Q}$, the field of rational numbers. It is a field extension of $\mathbb{Q}$ which is also a vector space of finite dimension over $\mathbb{Q}$. Since the elements of a number field are algebraic numbers, roots of a fixed polynomial $a_0 + a_1z + \ldots + z^n$ with integer coefficients, one calls them also algebraic number fields. The study of algebraic number fields is part of algebraic number theory.

Examples:
- quadratic fields: $\mathbb{Q}(\sqrt{d})$, where $d$ is a rational number. It is in general a field extension of degree 2 over the field of rational number.
- cyclotomic fields: $\mathbb{Q}(\zeta)$, where $\zeta$ is a $n$’th root of 1. It is a field extension of degree $\phi(n)$, where $\phi(n)$ is the Euler function.

Octonions

The octonions can be written as linear combinations of elements $e_0, e_1, e_2, \ldots, e_7$. The multiplication is determined by the multiplication table

<table>
<thead>
<tr>
<th>*</th>
<th>1</th>
<th>$e_1$</th>
<th>$e_2$</th>
<th>$e_3$</th>
<th>$e_4$</th>
<th>$e_5$</th>
<th>$e_6$</th>
<th>$e_7$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>$e_1$</td>
<td>$e_2$</td>
<td>$e_3$</td>
<td>$e_4$</td>
<td>$e_5$</td>
<td>$e_6$</td>
<td>$e_7$</td>
</tr>
<tr>
<td>$e_1$</td>
<td>$e_1$</td>
<td>$-1$</td>
<td>$e_4$</td>
<td>$e_7$</td>
<td>$-e_2$</td>
<td>$e_6$</td>
<td>$-e_5$</td>
<td>$-e_3$</td>
</tr>
<tr>
<td>$e_2$</td>
<td>$e_2$</td>
<td>$-e_4$</td>
<td>$-1$</td>
<td>$e_5$</td>
<td>$e_1$</td>
<td>$-e_3$</td>
<td>$e_7$</td>
<td>$-e_6$</td>
</tr>
<tr>
<td>$e_3$</td>
<td>$e_3$</td>
<td>$-e_7$</td>
<td>$-e_5$</td>
<td>$-1$</td>
<td>$e_6$</td>
<td>$e_2$</td>
<td>$-e_4$</td>
<td>$e_1$</td>
</tr>
<tr>
<td>$e_4$</td>
<td>$e_4$</td>
<td>$e_2$</td>
<td>$-e_1$</td>
<td>$-e_6$</td>
<td>$-1$</td>
<td>$e_7$</td>
<td>$e_3$</td>
<td>$-e_5$</td>
</tr>
<tr>
<td>$e_5$</td>
<td>$e_5$</td>
<td>$-e_6$</td>
<td>$e_3$</td>
<td>$-e_2$</td>
<td>$-e_7$</td>
<td>$-1$</td>
<td>$e_1$</td>
<td>$e_4$</td>
</tr>
<tr>
<td>$e_6$</td>
<td>$e_6$</td>
<td>$e_5$</td>
<td>$-e_7$</td>
<td>$e_4$</td>
<td>$-e_3$</td>
<td>$-e_1$</td>
<td>$-1$</td>
<td>$e_2$</td>
</tr>
<tr>
<td>$e_7$</td>
<td>$e_7$</td>
<td>$e_3$</td>
<td>$e_6$</td>
<td>$-e_1$</td>
<td>$e_5$</td>
<td>$-e_4$</td>
<td>$-e_2$</td>
<td>$-1$</td>
</tr>
</tbody>
</table>

Octonions are also called Cayley numbers. The multiplication of octonions is not associative. Octonions have been discovered by John T. Graves in 1843 and independently by Arthur Cayley.

Order

The order of a finite group is the set of elements in the group.

P-group

A p-group is a finite group with order $p^n$, where $p$ is a prime integer and $n > 0$. 
The quaternions can be written as linear combinations of elements $1, i, j, k$. The multiplication is determined by the multiplication table:

\[
\begin{array}{cccc}
\times & 1 & i & j & k \\
1 & 1 & i & j & k \\
i & i & -1 & k & -j \\
j & j & -k & -1 & i \\
k & k & j & -i & -1 \\
\end{array}
\]

Quaternions are useful to compute rotations in three dimensions.

A semigroup $(X, +)$ is a set $X$ with a binary operation $+$ which satisfies the associativity law $(a + b) + c = a + (b + c)$. Examples:

- a group is a semigroup.
- the set of finite words in an alphabet with composition form a semigroup $\text{word1} + \text{word2} = \text{word1word2}$
- the natural numbers form a semigroup under addition.

A commutative semigroup is a semigroup $(X, +)$ which is commutative. $a + b = b + a$.

- the natural numbers form a commutative semigroup under addition.
- composition of words over a finite alphabet form a noncommutative semigroup

The kernel of a homomorphism between two groups $G, H$ is the set of all elements in $G$ which are mapped to the zero element of $H$. For example, $\text{SL}(n, R)$ is the kernel of the homomorphism from $\text{GL}(n, R)$ to $R \setminus \{0\}$ defined by $\phi(A) = \det(A)$.

A subgroup of a group $G$ is a subset of $G$ which is also a group. Examples:

- the set of $n \times n$ matrices with determinant 1 is a subgroup of the set of $n \times n$ matrices with nonzero determinant.
- the trivial subgroup $\{0\}$ is always a subgroup of a group $(G, *, 0)$. 
Theorem of Cauchy

Theorem of Cauchy in group theory states that every finite group whose order is divisible by a prime number \( p \) contains a subgroup of order \( p \).

Sedenions

Sedenions form a zero Divisor Algebra. By a theorem of Frobenius (1877), there are three and only three associative finite division algebras: the real numbers \( \mathbb{R} \), the complex numbers \( \mathbb{C} \) and the quaternions \( \mathbb{Q} \). Similar algebras in higher dimensions have zero divisors: sedenions are examples.

Field

A field is a commutative ring \((R, +, *, 0, 1)\) such that \((R, +, 0)\) and \((R \setminus 0, *, 1)\) are both commutative groups.

Theorem of Zorn

By a theorem of Zorn (1933), every alternative, quadratic, real non-associative algebra without zero divisors is isomorphic to the 8-dimensional octonions \( O \).

Theorem of Hurwitz

Theorem of Hurwitz: the normed composition algebras with unit are: real numbers, complex numbers, quaternions; and octonions.

Theorem of Kervaire and Milnor

Theorem of Kervaire and Milnor: In 1958, Kervaire and Milnor proved independently of each other that the finite-dimensional real division algebras have dimensions 1, 2, 4, or 8.

Theorem of Adams

Theorem of Adams: In 1960, Adams proved that a continuous multiplication in \( \mathbb{R}^{n+1} \) with two-sided unit and with norm product exists only for \( n + 1 = 1, 2, 4, \) or 8.
Theorem of Hurwitz

[Theorem of Hurwitz]: the normed composition algebras with unit are:

- real numbers
- complex numbers
- quaternions
- octonions

Theorems of Sylov

[Theorems of Sylov] If $G$ is a finite group of order $|G| = p^n q$, where $p$ is a prime number, then $G$ has a subgroup of order $p^n$. Such groups are called Sylov groups and all of them are isomorphic. Furthermore, the number $N$ of different $p$-Sylov groups in $G$ satisfies $N = 1 \mod(p)$.

This file is part of the Sofia project sponsored by the Provost’s fund for teaching and learning at Harvard university. There are 39 entries in this file.
Index
additive, 1
algebra, 1
alternating group, 1
An algebraic number field, 1
Artinian module, 1
Artinian ring, 1
Cayley’s theorem, 2
center, 2
commutative group, 4
commutative ring, 4
commutative semigroup, 6
commutator, 2
commutator subgroup, 2
factor group, 2
field, 7
finite group, 2
function field, 4
group, 3
homomorphism, 4
isomorphism, 4
kernel, 6
normal subgroup, 3
number field, 5
octonions, 5
order, 5
p-group, 5
quaterions, 6
ring, 3
sedenions, 7
semigroup, 6
subgroup, 6
Theorem of Adams, 7
Theorem of Cauchy, 7
Theorem of Hurwitz, 7, 8
Theorem of Kervaire and Milnor, 7
theorem of Zorn, 7
Theorems of Sylov, 8