

Abelian group

In abstract algebra, an **abelian group**, also called a **commutative group**, is a group in which the result of applying the group operation to two group elements does not depend on their order (the axiom of commutativity). Abelian groups generalize the arithmetic of addition of integers. They are named after Niels Henrik Abel.^[1]

The concept of an abelian group is one of the first concepts encountered in undergraduate abstract algebra, with many other basic objects, such as a module and a vector space, being its refinements. The theory of abelian groups is generally simpler than that of their non-abelian counterparts, and finite abelian groups are very well understood. On the other hand, the theory of infinite abelian groups is an area of current research.

Definition

An abelian group is a set, A , together with an operation " \bullet " that combines any two elements a and b to form another element denoted $a \bullet b$. The symbol " \bullet " is a general placeholder for a concretely given operation. To qualify as an abelian group, the set and operation, (A, \bullet) , must satisfy five requirements known as the *abelian group axioms*:

Closure

For all a, b in A , the result of the operation $a \bullet b$ is also in A .

Associativity

For all a, b and c in A , the equation $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ holds.

Identity element

There exists an element e in A , such that for all elements a in A , the equation $e \bullet a = a \bullet e = a$ holds.

Inverse element

For each a in A , there exists an element b in A such that $a \bullet b = b \bullet a = e$, where e is the identity element.

Commutativity

For all a, b in A , $a \bullet b = b \bullet a$.

More compactly, an abelian group is a commutative group. A group in which the group operation is not commutative is called a "non-abelian group" or "non-commutative group".

Facts

Notation

There are two main notational conventions for abelian groups — additive and multiplicative.

Convention	Operation	Identity	Powers	Inverse
Addition	$x + y$	0	nx	$-x$
Multiplication	$x * y$ or xy	e or 1	x^n	x^{-1}

Generally, the multiplicative notation is the usual notation for groups, while the additive notation is the usual notation for modules. The additive notation may also be used to emphasize that a particular group is abelian, whenever both abelian and non-abelian groups are considered.

Multiplication table

To verify that a finite group is abelian, a table (matrix) - known as a Cayley table - can be constructed in a similar fashion to a multiplication table. If the group is $G = \{g_1 = e, g_2, \dots, g_n\}$ under the operation \cdot , the (i, j) 'th entry of this table contains the product $g_i \cdot g_j$. The group is abelian if and only if this table is symmetric about the main diagonal (i.e. if the matrix is a symmetric matrix).

This is true since if the group is abelian, then $g_i \cdot g_j = g_j \cdot g_i$. This implies that the (i, j) 'th entry of the table equals the (j, i) 'th entry - i.e. the table is symmetric about the main diagonal.

Examples

- For the integers and the operation addition "+", denoted $(\mathbf{Z}, +)$, the operation + combines any two integers to form a third integer, addition is associative, zero is the additive identity, every integer n has an additive inverse, $-n$, and the addition operation is commutative since $m + n = n + m$ for any two integers m and n .
- Every cyclic group G is abelian, because if x, y are in G , then $xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$. Thus the integers, \mathbf{Z} , form an abelian group under addition, as do the integers modulo n , $\mathbf{Z}/n\mathbf{Z}$.
- Every ring is an abelian group with respect to its addition operation. In a commutative ring the invertible elements, or units, form an abelian multiplicative group. In particular, the real numbers are an abelian group under addition, and the nonzero real numbers are an abelian group under multiplication.
- Every subgroup of an abelian group is normal, so each subgroup gives rise to a quotient group. Subgroups, quotients, and direct sums of abelian groups are again abelian.

In general, matrices, even invertible matrices, do not form an abelian group under multiplication because matrix multiplication is generally not commutative. However, some groups of matrices are abelian groups under matrix multiplication - one example is the group of 2x2 rotation matrices.

Historical remarks

Abelian groups were named for Norwegian mathematician Niels Henrik Abel by Camille Jordan because Abel found that the commutativity of the group of an equation implies its roots are solvable by radicals. See Section 6.5 of Cox (2004) for more information on the historical background.

Properties

If n is a natural number and x is an element of an abelian group G written additively, then nx can be defined as $x + x + \dots + x$ (n summands) and $(-n)x = -(nx)$. In this way, G becomes a module over the ring \mathbf{Z} of integers. In fact, the modules over \mathbf{Z} can be identified with the abelian groups.

Theorems about abelian groups (i.e. modules over the principal ideal domain \mathbf{Z}) can often be generalized to theorems about modules over an arbitrary principal ideal domain. A typical example is the classification of finitely generated abelian groups which is a specialization of the structure theorem for finitely generated modules over a principal ideal domain. In the case of finitely generated abelian groups, this theorem guarantees that an abelian group splits as a direct sum of a torsion group and a free abelian group. The former may be written as a direct sum of finitely many groups of the form $\mathbf{Z}/p^k\mathbf{Z}$ for p prime, and the latter is a direct sum of finitely many copies of \mathbf{Z} .

If $f, g : G \rightarrow H$ are two group homomorphisms between abelian groups, then their sum $f + g$, defined by $(f + g)(x) = f(x) + g(x)$, is again a homomorphism. (This is not true if H is a non-abelian group.) The set $\text{Hom}(G, H)$ of all group homomorphisms from G to H thus turns into an abelian group in its own right.

Somewhat akin to the dimension of vector spaces, every abelian group has a *rank*. It is defined as the cardinality of the largest set of linearly independent elements of the group. The integers and the rational numbers have rank one, as well as every subgroup of the rationals.

Finite abelian groups

Cyclic groups of integers modulo n , $\mathbf{Z}/n\mathbf{Z}$, were among the first examples of groups. It turns out that an arbitrary finite abelian group is isomorphic to a direct sum of finite cyclic groups of prime power order, and these orders are uniquely determined, forming a complete system of invariants. The automorphism group of a finite abelian group can be described directly in terms of these invariants. The theory had been first developed in the 1879 paper of Georg Frobenius and Ludwig Stickelberger and later was both simplified and generalized to finitely generated modules over a principal ideal domain, forming an important chapter of linear algebra.

Classification

The **fundamental theorem of finite abelian groups** states that every finite abelian group G can be expressed as the direct sum of cyclic subgroups of prime-power order. This is a special case of the fundamental theorem of finitely generated abelian groups when G has zero rank.

The cyclic group \mathbf{Z}_{mn} of order mn is isomorphic to the direct sum of \mathbf{Z}_m and \mathbf{Z}_n if and only if m and n are coprime. It follows that any finite abelian group G is isomorphic to a direct sum of the form

$$\mathbf{Z}_{k_1} \oplus \cdots \oplus \mathbf{Z}_{k_u}$$

in either of the following canonical ways:

- the numbers k_1, \dots, k_u are powers of primes
- k_1 divides k_2 , which divides k_3 , and so on up to k_u .

For example, \mathbf{Z}_{15} can be expressed as the direct sum of two cyclic subgroups of order 3 and 5: $\mathbf{Z}_{15} \cong \{0, 5, 10\} \oplus \{0, 3, 6, 9, 12\}$. The same can be said for any abelian group of order 15, leading to the remarkable conclusion that all abelian groups of order 15 are isomorphic.

For another example, every abelian group of order 8 is isomorphic to either \mathbf{Z}_8 (the integers 0 to 7 under addition modulo 8), $\mathbf{Z}_4 \oplus \mathbf{Z}_2$ (the odd integers 1 to 15 under multiplication modulo 16), or $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$.

See also list of small groups for finite abelian groups of order 16 or less.

Automorphisms

One can apply the fundamental theorem to count (and sometimes determine) the automorphisms of a given finite abelian group G . To do this, one uses the fact (which will not be proved here) that if G splits as a direct sum $H \oplus K$ of subgroups of coprime order, then $\text{Aut}(H \oplus K) \cong \text{Aut}(H) \oplus \text{Aut}(K)$.

Given this, the fundamental theorem shows that to compute the automorphism group of G it suffices to compute the automorphism groups of the Sylow p -subgroups separately (that is, all direct sums of cyclic subgroups, each with order a power of p). Fix a prime p and suppose the exponents e_i of the cyclic factors of the Sylow p -subgroup are arranged in increasing order:

$$e_1 \leq e_2 \leq \cdots \leq e_n$$

for some $n > 0$. One needs to find the automorphisms of

$$\mathbf{Z}_{p^{e_1}} \oplus \cdots \oplus \mathbf{Z}_{p^{e_n}}.$$

One special case is when $n = 1$, so that there is only one cyclic prime-power factor in the Sylow p -subgroup P . In this case the theory of automorphisms of a finite cyclic group can be used. Another special case is when n is arbitrary but $e_i = 1$ for $1 \leq i \leq n$. Here, one is considering P to be of the form

$$\mathbf{Z}_p \oplus \cdots \oplus \mathbf{Z}_p,$$

so elements of this subgroup can be viewed as comprising a vector space of dimension n over the finite field of p elements \mathbb{F}_p . The automorphisms of this subgroup are therefore given by the invertible linear transformations, so

$$\text{Aut}(P) \cong \text{GL}(n, \mathbb{F}_p),$$

where GL is the appropriate general linear group. This is easily shown to have order

$$|\text{Aut}(P)| = (p^n - 1) \cdots (p^n - p^{n-1}).$$

In the most general case, where the e_i and n are arbitrary, the automorphism group is more difficult to determine. It is known, however, that if one defines

$$d_k = \max\{r | e_r = e_k\}$$

and

$$c_k = \min\{r | e_r = e_k\}$$

then one has in particular $d_k \geq k$, $c_k \leq k$, and

$$|\text{Aut}(P)| = \left(\prod_{k=1}^n p^{d_k} - p^{k-1} \right) \left(\prod_{j=1}^n (p^{e_j})^{n-d_j} \right) \left(\prod_{i=1}^n (p^{e_i-1})^{n-c_i+1} \right).$$

One can check that this yields the orders in the previous examples as special cases (see [Hillar,Rhea]).

Infinite abelian groups

The simplest infinite abelian group is the infinite cyclic group \mathbf{Z} . Any finitely generated abelian group A is isomorphic to the direct sum of r copies of \mathbf{Z} and a finite abelian group, which in turn is decomposable into a direct sum of finitely many cyclic groups of primary orders. Even though the decomposition is not unique, the number r , called the **rank** of A , and the prime powers giving the orders of finite cyclic summands are uniquely determined.

By contrast, classification of general infinitely generated abelian groups is far from complete. Divisible groups, i.e. abelian groups A in which the equation $nx = a$ admits a solution $x \in A$ for any natural number n and element a of A , constitute one important class of infinite abelian groups that can be completely characterized. Every divisible group is isomorphic to a direct sum, with summands isomorphic to \mathbf{Q} and Prüfer groups \mathbf{Q}/\mathbf{Z} for various prime numbers p , and the cardinality of the set of summands of each type is uniquely determined.^[2] Moreover, if a divisible group A is a subgroup of an abelian group G then A admits a direct complement: a subgroup C of G such that $G = A \oplus C$. Thus divisible groups are injective modules in the category of abelian groups, and conversely, every injective abelian group is divisible (Baer's criterion). An abelian group without non-zero divisible subgroups is called **reduced**.

Two important special classes of infinite abelian groups with diametrically opposite properties are *torsion groups* and *torsion-free groups*, exemplified by the groups \mathbf{Q}/\mathbf{Z} (periodic) and \mathbf{Q} (torsion-free).

Torsion groups

An abelian group is called **periodic** or **torsion** if every element has finite order. A direct sum of finite cyclic groups is periodic. Although the converse statement is not true in general, some special cases are known. The first and second Prüfer theorems state that if A is a periodic group and either it has **bounded exponent**, i.e. $nA = 0$ for some natural number n , or if A is countable and the p -heights of the elements of A are finite for each p , then A is isomorphic to a direct sum of finite cyclic groups.^[3] The cardinality of the set of direct summands isomorphic to $\mathbf{Z}/p^m\mathbf{Z}$ in such a decomposition is an invariant of A . These theorems were later subsumed in the **Kulikov criterion**. In a different direction, Helmut Ulm found an extension of the second Prüfer theorem to countable abelian p -groups with elements of infinite height: those groups are completely classified by means of their Ulm invariants.

Torsion-free and mixed groups

An abelian group is called **torsion-free** if every non-zero element has infinite order. Several classes of torsion-free abelian groups have been extensively studied:

- Free abelian groups, i.e. arbitrary direct sums of \mathbf{Z}
- Cotorsion and algebraically compact torsion-free groups such as the p -adic integers
- Slender groups

An abelian group that is neither periodic nor torsion-free is called **mixed**. If A is an abelian group and $T(A)$ is its torsion subgroup then the factor group $A/T(A)$ is torsion-free. However, in general the torsion subgroup is not a direct summand of A , so the torsion-free factor cannot be realized as a subgroup of A and A is *not* isomorphic to $T(A) \oplus A/T(A)$. Thus the theory of mixed groups involves more than simply combining the results about periodic and torsion-free groups.

Invariants and classification

One of the most basic invariants of an infinite abelian group A is its rank: the cardinality of the maximal linearly independent subset of A . Abelian groups of rank 0 are precisely the periodic groups, while torsion-free abelian groups of rank 1 are necessarily subgroups of \mathbf{Q} and can be completely described. More generally, a torsion-free abelian group of finite rank r is a subgroup of \mathbf{Q}^r . On the other hand, the group of p -adic integers \mathbf{Z}_p is a torsion-free abelian group of infinite \mathbf{Z} -rank and the groups \mathbf{Z}_p^n with different n are non-isomorphic, so this invariant does not even fully capture properties of some familiar groups.

The classification theorems for finitely generated, divisible, countable periodic, and rank 1 torsion-free abelian groups explained above were all obtained before 1950 and form a foundation of the classification of more general infinite abelian groups. Important technical tools used in classification of infinite abelian groups are pure and basic subgroups. Introduction of various invariants of torsion-free abelian groups has been one avenue of further progress. See the books by Irving Kaplansky, László Fuchs, Phillip Griffiths, and David Arnold, as well as the proceedings of the conferences on Abelian Group Theory published in Lecture Notes in Mathematics for more recent results.

Additive groups of rings

The additive group of a ring is an abelian group, but not all abelian groups are additive groups of rings (with nontrivial multiplication). Some important topics in this area of study are:

- Tensor product
- Corner's results on countable torsion-free groups
- Shelah's work to remove cardinality restrictions

Relation to other mathematical topics

Many large abelian groups possess a natural topology, which turns them into topological groups.

The collection of all abelian groups, together with the homomorphisms between them, forms the category \mathbf{Ab} , the prototype of an abelian category.

Nearly all well-known algebraic structures other than Boolean algebras, are undecidable. Hence it is surprising that Tarski's student Szmielew (1955) proved that the first order theory of abelian groups, unlike its nonabelian counterpart, is decidable. This decidability, plus the fundamental theorem of finite abelian groups described above, highlight some of the successes in abelian group theory, but there are still many areas of current research:

- Amongst torsion-free abelian groups of finite rank, only the finitely generated case and the rank 1 case are well understood;
- There are many unsolved problems in the theory of infinite-rank torsion-free abelian groups;

- While countable torsion abelian groups are well understood through simple presentations and Ulm invariants, the case of countable mixed groups is much less mature.
- Many mild extensions of the first order theory of abelian groups are known to be undecidable.
- Finite abelian groups remain a topic of research in computational group theory.

Moreover, abelian groups of infinite order lead, quite surprisingly, to deep questions about the set theory commonly assumed to underlie all of mathematics. Take the Whitehead problem: are all Whitehead groups of infinite order also free abelian groups? In the 1970s, Saharon Shelah proved that the Whitehead problem is:

- Undecidable in ZFC, the conventional axiomatic set theory from which nearly all of present day mathematics can be derived. The Whitehead problem is also the first question in ordinary mathematics proved undecidable in ZFC;
- Undecidable even if ZFC is augmented by taking the generalized continuum hypothesis as an axiom;
- Decidable if ZFC is augmented with the axiom of constructibility (see statements true in L).

A note on the typography

Among mathematical adjectives derived from the proper name of a mathematician, the word "abelian" is rare in that it is often spelled with a lowercase **a**, rather than an uppercase **A**, indicating how ubiquitous the concept is in modern mathematics.^[4]

Notes

[1] Jacobson (2009), p. 41

[2] For example, $\mathbf{Q}/\mathbf{Z} \cong \sum_p \mathbf{Q}/\mathbf{Z}_p$.

[3] Countability assumption in the second Prüfer theorem cannot be removed: the torsion subgroup of the direct product of the cyclic groups $\mathbf{Z}/p^m\mathbf{Z}$ for all natural m is not a direct sum of cyclic groups.

[4] Abel Prize Awarded: The Mathematicians' Nobel (http://www.maa.org/devlin/devlin_04_04.html)

References

- Cox, David (2004) *Galois Theory*. Wiley-Interscience. Hoboken, NJ. xx+559 pp. MR2119052
- Fuchs, László (1970) *Infinite abelian groups, Vol. I*. Pure and Applied Mathematics, Vol. 36. New York–London: Academic Press. xi+290 pp. MR0255673
- ----- (1973) *Infinite abelian groups, Vol. II*. Pure and Applied Mathematics. Vol. 36-II. New York–London: Academic Press. ix+363 pp. MR0349869
- Griffith, Phillip A. (1970). *Infinite Abelian group theory*. Chicago Lectures in Mathematics. University of Chicago Press. ISBN 0-226-30870-7.
- I.N. Herstein (1975), *Topics in Algebra*, 2nd edition (John Wiley and Sons, New York) ISBN 0-471-02371-X
- Hillar, Christopher and Rhea, Darren (2007), Automorphisms of finite abelian groups. *Amer. Math. Monthly* **114**, no. 10, 917-923. arXiv:0605185.
- Jacobson, Nathan (2009). *Basic algebra*. **1** (2nd ed.). Dover. ISBN 978-0-486-47189-1..
- Szmielew, Wanda (1955) "Elementary properties of abelian groups," *Fundamenta Mathematica* **41**: 203-71.

Article Sources and Contributors

Abelian group *Source:* <http://en.wikipedia.org/w/index.php?oldid=428592415> *Contributors:* 128.111.201.xxx, Aeons, Amire80, Andres, Andyparkerson, Arcfrk, AxelBoldt, Bender2k14, Brighterorange, Brona, Bryan Derksen, CRGreathouse, Charles Matthews, Chas zzz brown, Chowbok, Ciphers, Coleegu, Conversion script, DHN, DL144, Dcoetzee, Diego Moya, Doradus, Dr Caligari, Drbreznjev, Drgruppenpest, Drilnoth, Dysprosia, Fibonacci, Fropuff, GB fan, Gandalf61, Gauge, Geschichte, Gifflite, Gregbard, Grubber, Helder.wiki, Isnow, JackSchmidt, Jdforrester, Jitse Niesen, Jlaire, Joe Campbell, Johnunq, Jonathans, Jorend, Kaoru Itou, Karada, Keenan Pepper, Konradek, Lagelspeil, Leonard G., Lethe, Lovro, Madmath789, Magic in the night, Mathisreallycool, Mets501, Michael Hardy, Michael Slone, Mikael V, Namwob0, Negi(afk), Newone, Oleg Alexandrov, Oli Filth, Pakaran, Patrick, Philosophygeek, Pmanderson, Poor Yorick, Quotient group, R.e.b., Recognizance, Revolver, Rickterp, Romann, Salix alba, Saxbryn, Schneelocke, SetaLyas, Shenme, Silly rabbit, SirJective, Ste4k, Stevertigo, Stifle, TakuyaMurata, Tango, Theresa knott, Tobias Bergemann, Topology Expert, Trhaynes, Vanish2, Vaughan Pratt, Vipul, Waltpohl, Warut, Zabadook, Zundark, 91 anonymous edits

License

Creative Commons Attribution-Share Alike 3.0 Unported
<http://creativecommons.org/licenses/by-sa/3.0/>