WIKIPEDIA

Principal ideal

In the mathematical field of ring theory, a **principal ideal** is an ideal I in a ring R that is generated by a single element a of R through multiplication by every element of R. The term also has another, similar meaning in order theory, where it refers to an (order) ideal in a poset P generated by a single element x of P, which is to say the set of all elements less than or equal to x in P.

The remainder of this article addresses the ring-theoretic concept.

Contents

Definitions

- a *left principal ideal* of R is a subset of R of the form $Ra = \{ra : r \text{ in } R\}$;
- a *right principal ideal* is a subset of the form $aR = \{ar : r \text{ in } R\}$;
- a *two-sided principal ideal* is a subset of all finite sums of elements of the form ras, namely, $RaR = \{r_1as_1 + ... + r_nas_n : r_1,s_1,...,r_n,s_n \text{ in } R\}$.

While this definition for two-sided principal ideal may seem to contrast with the others, it is necessary to ensure that the ring remains closed under addition.

If R is a commutative ring, then the above three notions are all the same. In that case, it is common to write the ideal generated by a as $\langle a\rangle$.

Examples of non-principal ideal

Not all ideals are principal. For example, consider the commutative ring $\mathbf{C}[x,y]$ of all polynomials in two variables x and y, with complex coefficients. The ideal $\langle x,y\rangle$ generated by x and y, which consists of all the polynomials in $\mathbf{C}[x,y]$ that have zero for the constant term, is not principal. To see this, suppose that p were a generator for $\langle x,y\rangle$; then x and y would both be divisible by p, which is impossible unless p is a nonzero constant. But zero is the only constant in $\langle x,y\rangle$, so we have a contradiction.

In the ring $Z[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in Z\}$, numbers in which a + b is even form a non-principal ideal. This ideal forms a regular hexagonal lattice in the complex plane. Consider (a,b) = (2,0) and (1,1). These numbers are elements of this ideal with the same norm (2), but because the only units in the ring are 1 and -1, they are not associates.

Examples of principal ideal

The principal ideals in Z are of the form $(n) = nZ$. Actually, every ideal I in Z is principal, which can be shown in the following way. Suppose $I = \langle n_1, n_2, \cdots \rangle$ where $n_1 \neq 0$, then consider the surjective homomorphisms $Z/\langle n_1 \rangle \to Z/\langle n_1, n_2 \rangle \to Z/\langle n_1, n_2, n_3 \rangle \to \cdots$. Since $Z/\langle n_1 \rangle$ is finite, for sufficiently large k $Z/\langle n_1, n_2, \cdots, n_k \rangle = Z/\langle n_1, n_2, \cdots, n_{k+1} \rangle = \cdots$. Thus, $I = \langle n_1, n_2, \cdots, n_k \rangle$, which implies I is always finitely generated. Since the ideal generated by any integers a and b, $\langle a, b \rangle$, is exactly $\langle \gcd(a, b) \rangle$, by induction on the number of generators, it follows that I is principal.

However, all rings have principal ideals, namely, any ideal generated by exactly one element. For example, the ideal $\langle x \rangle$ is a principal ideal of $C[x, y]$, and {\di is a principal ideal of {\disp. In fact, {\dis and {\disp are principal ideals of any ring .

Related definitions

A ring in which every ideal is principal is called *principal*, or a principal ideal ring. A principal ideal domain (PID) is an integral domain in which every ideal is principal. Any PID must be a unique factorization domain; the normal proof of unique factorization in the integers (the so-called fundamental theorem of arithmetic) holds in any PID.

Properties

Any Euclidean domain is a PID; the algorithm used to calculate greatest common divisors may be used to find a generator of any ideal. More generally, any two principal ideals in a commutative ring have a greatest common divisor in the sense of ideal multiplication. In principal ideal domains, this allows us to calculate greatest common divisors of elements of the ring, up to multiplication by a unit; we define gcd(*a*,*b*) to be any generator of the ideal ⟨*a*,*b*⟩.

For a Dedekind domain *R*, we may also ask, given a non-principal ideal *I* of *R*, whether there is some extension *S* of *R* such that the ideal of *S* generated by *I* is principal (said more loosely *I becomes principal* in *S*). This question arose in connection with the study of rings of algebraic integers (which are examples of Dedekind domains) in number theory, and led to the development of class field theory by Teiji Takagi, Emil Artin, David Hilbert, and many others.

The principal ideal theorem of class field theory states that every integer ring *R* (i.e. the ring of integers of some number field) is contained in a larger integer ring *S* which has the property that *every* ideal of *R* becomes a principal ideal of *S*. In this theorem we may take *S* to be the ring of integers of the Hilbert class field of *R*; that is, the maximal unramified abelian extension (that is, Galois extension whose Galois group is abelian) of the fraction field of *R*, and this is uniquely determined by *R*.

Krull's principal ideal theorem states that if *R* is a Noetherian ring and *I* is a principal, proper ideal of *R*, then *I* has height at most one.

See also

- Ascending chain condition for principal ideals

References

- Gallian, Joseph A. (2017). *Contemporary Abstract Algebra* (9th ed.). Cengage Learning. ISBN 978-1-305-65796-0.