ALGEBRAIC STRUCTURES

JERRY SUN

1. Modules and Rings

1.1. **Modules.** A module is one of the main algebraic structures in abstract algebra. A module over a ring is a generalization of the notion of vector space over a field, wherein the corresponding scalars are the elements of an arbitrary given ring (with identity) and a multiplication (on the left and/or on the right) is defined between elements of the ring and elements of the module. A module taking its scalars from a ring R is called an R-module. The reason why a module over a ring is a generalization of a vector space over a field, is because a ring has less operations then a field and therefore is less restrictive.

A module is an additive abelian group just like in a vector space. A product is defined between elements of the ring and elements of the module that is distributive over the addition operation of each parameter and is compatible with the ring multiplication. Modules also may or may not have a basis or be decomposable into smaller modules.

Modules are very closely related to the representation theory of groups. They are also one of the central notions of commutative algebra and homological algebra, and are used widely in algebraic geometry and algebraic topology.

1.2. **Rings.** A ring is another one of the main algebraic structures used in abstract algebra. It consists of a set equipped with two binary operations that generalize the arithmetic operations of addition and multiplication. Through this generalization, theorems from arithmetic are extended to non-numerical objects such as polynomials, series, matrices and functions. A ring is an abelian group with a second binary operation that is associative, is distributive over the abelian group operation, and has an identity element (although sometimes we do not require it to have an identity). Just like with the integers, the abelian group operation is called addition and the second binary operation is called multiplication.
Whether a ring is commutative or not (the order in which you multiply two elements doesn't matter) changes the way the ring behaves. Hence, ring theory is broken up into branches depending on if the ring is commutative. the development of ring theory has been influenced a lot by problems in algebraic geometry and algebriac number theory.

2. Definitions

2.1. **Ring.** A ring is a set R equipped with two binary operations + and $\cdot$ satisfying the following three sets of axioms, called the ring axioms

(1) R is an abelian group under addition, meaning that: $(a + b) + c = a + (b + c)$ for all a, b, c in R (that is, + is associative).

$$a + b = b + a$$

Date: June 6, 2020.

for all a, b in R (that is, + is commutative). There is an element 0 in R such that a + 0 = a for all a in R (that is, 0 is the additive identity). For each a in R there exists a in R such that $a + (a) = 0$ (that is, a is the additive inverse of a).

(2) R is a monoid under multiplication, meaning that:

$$(ab)c = a(bc)$$

for all a, b, c in R (that is, $\cdot$ is associative). There is an element 1 in R such that $a1 = a$ and $1a = a$ for all a in R (that is, 1 is the multiplicative identity).[5]

(3) Multiplication is distributive with respect to addition, meaning that: $a(b + c) = (ab) + (ac)$ for all a, b, c in R (left distributivity). $(b + c)a = (ba) + (ca)$ for all a, b, c in R (right distributivity).

2.2. **Module.** Suppose that R is a ring and 1R is its multiplicative identity. A left R-module M consists of an abelian group (M, +) and an operation : R × M → M such that for all r, s in R and x, y in M, we have:

(a) $r * (x + y) = rx + ry$
(b) $(r + s) * x = rx + rs$
(c) $(rs) * x = r * (sx)$
(d) $1_r * x = x$

3. Examples of Modules and Rings

3.1. **Modules.**

(a) IfK is a field, then K-vector spaces (vector spaces over K) and K-modules are identical.
(b) If K is a field, and $K[x]$ a univariate polynomial ring, then a K[x]-module M is a K-module with an additional action of x on M that commutes with the action of K on M. In other words, a K[x]-module is a K-vector space M combined with a linear map from M to M. Applying the Structure theorem for finitely generated modules over a principal ideal domain to this example shows the existence of the rational and Jordan canonical forms.
(c) If R is any ring and I is any left ideal in R, then I is a left R-module, and analogously right ideals in R are right R-modules.

3.2. **Rings.**

(a) The integers modulo 4
(b) The set of 2-by-2 matrices with real number entries is written
(c) Any algebra over a field.
(d) The Gaussian Integers
(e) Any algebra over a field.
(f) The polynomial ring $R[X]$ of polynomials over a ring R is itself a ring. A free module over R of infinite dimension.

4. Operations

4.1. **Direct Sums and Direct Products.** In this section, we will talk about two operations to combine two or more algebraic structures, the direct sum and the direct product.

The direct sum is an operation to combine two objects, not necessarily an algebraic

structure. For example, the direct sum $\mathbf{R} \oplus \mathbf{R}$, where $\mathbf{R}$ is real coordinate space, is the Cartesian plane, $\mathbf{R}^2$. For algebraic structures the direct sum is similar. The direct sum of two abelian groups A and B is another abelian group $A \oplus B$ consisting of the ordered pairs (a, b) where $\in A$ and $b \in B$. (Confusingly this ordered pair is also called the cartesian product of the two groups.) To add ordered pairs, we define the sum $(a, b) + (c, d)$ to be $(a + c, b + d)$; in other words addition is defined coordinate-wise. A similar process can be used to form the direct sum of any two algebraic structures, such as rings, modules, and vector spaces.

We can also form direct sums with any finite number of summands, for example $A \oplus B \oplus C$, provided A, B, and C are the same kinds of algebraic structures (that is, all groups, rings, vector spaces, etc.). This relies on the fact that the direct sum is associative up to isomorphism. That is, $(A \oplus B) \oplus C \cong A \oplus (B \oplus C)$ for any algebraic structures A, B, and C of the same kind. The direct sum is also commutative up to isomorphism, i.e. $A \oplus B \cong B \oplus A$ for any algebraic structures A and B of the same kind.

If we are only adding a finite amount of objects then the direct sum and the direct product are the same and can be used interchangeably, however if the operation used to combine is + then we would call it a direct sum and if it is a product we use direct product.

However, when there are an infinite amount of summands the direct product and direct sum mean different things

4.2. **Subrings.** A subset S of R is a subring if it still satisfies all the the conditions for rings while being restricted to the elements in s instead of R.. Equivalently, S is a subring if it is not empty, and for any x, y in S,xy, x+y and -x are in S. If all rings have been assumed, by convention, to have a multiplicative identity, then to be a subring,we would also require S to share the same identity element as R. So if all rings have been assumed to have a multiplicative identity, then a proper ideal is not a subring.

For example, the ring Z of integers is a subring of the field of real numbers and also a subring of the ring of polynomials Z[X] (in both cases, Z contains 1, which is the multiplicative identity of the larger rings). On the other hand, the subset of even integers 2Z does not contain the identity element 1 and thus does not qualify as a subring of Z.

4.2.1. *Submodules.* Suppose M is a left R-module and N is a subgroup of M. Then N is a submodule (or more explicitly an R-submodule) if for any n in N and any r in R, the product r n is in N (or n r for a right R-module).

4.3. **Ideals.** In ring theory,, an ideal is a special subset of a ring. Ideals generalize certain subsets of the integers, such as the even numbers or the multiples of 3. Addition and subtraction of even numbers preserves evenness, and multiplying an even number by any other integer results in another even number; these closure and absorption properties are the defining properties of an ideal. An ideal can be used to construct a quotient ring similarly to the way that, in group theory, a normal subgroup can be used to construct a quotient group. It is very similar in that quotient groups are "modding out" some of the elements, the ideal is too.

The ideals may be distinct from the ring elements, and certain properties of integers, when generalized to rings, attach more naturally to the ideals than to the elements of the ring. For instance, the prime ideals of a ring are analogous to prime numbers, and the Chinese remainder theorem can be generalized to ideals. There is a version of unique prime factorization for the ideals of a Dedekind domain (a type of ring important in number theory). The difference between a subring and an ideal is that the subring is closed under multiplication with elements inside the subring while ideals are closed under mutliplication of an element in the ideal and an element in the ring.

5. Terminology and other definitions

5.1. **Types of Rings and Modules.**

5.1.1. *Module Types.*

(a) Finitely generated
An R-module M is finitely generated if there exist finitely many elements x1, ..., xn in M such that every element of M is a linear combination of those elements with coefficients from the ring R.

(b) Cyclic
A module is called a cyclic module if it is generated by one element. Free A free R-module is a module that has a basis, or equivalently, one that is isomorphic to a direct sum of copies of the ring R. These are the modules that behave very much like vector spaces.

(c) Simple
A simple module S is a module that is not 0 and whose only submodules are 0 and S. Simple modules are sometimes called irreducible.[5]

(d) Semisimple
A semisimple module is a direct sum (finite or not) of simple modules. Historically these modules are also called completely reducible.

(e) Indecomposable
An indecomposable module is a non-zero module that cannot be written as a direct sum of two non-zero submodules. Every simple module is indecomposable, but there are indecomposable modules which are not simple (e.g. uniform modules).

(f) Torsion-free:
A torsion-free module is a module over a ring such that 0 is the only element annihilated by a regular element (non zero-divisor) of the ring, equivalently rm=0 implies r=0 or m=0.

(g) Noetherian
A Noetherian module is a module which satisfies the ascending chain condition on submodules, that is, every increasing chain of submodules becomes stationary after finitely many steps. Equivalently, every submodule is finitely generated.

(h) Artinian
An Artinian module is a module which satisfies the descending chain condition on submodules, that is, every decreasing chain of submodules becomes stationary after finitely many steps.

5.1.2. *Rings Types.*

(a) Division ring: A division ring is a ring such that every non-zero element is a unit. An invertible element or a unit in a ring with identity R is any element u that has an inverse element in the multiplicative monoid of R, i.e. an element v such that
$uv = vu = 1R$, where $1R$ is the multiplicative identity.)

(b) Domains: A nonzero ring with no nonzero zero-divisors is called a domain. A commutative domain is called an integral domain. The most important integral domains are principal ideals domains, PID for short, and fields. A principal ideal domain is an integral domain in which every ideal is principal. These rings arise in number theoy when we are studying the prime factorizations in general number fields

References

[1] https://ocw.mit.edu/courses/mathematics/18-703-modern-algebra-spring-2013/lecture-notes/MIT18$_7$03S13$_p$ra_{l1}0.*pdf*

[2] https://en.wikipedia.org/wiki/Ring$_(mathematics)$

[3] https://en.wikipedia.org/wiki/Module$_(mathematics)$

Palo Alto, CA 94306
Email address: jsun5047@gmail.com