普林斯顿数学指南

1° Groups

2° Fields ~ number systems

one binary operation

addition and multiplication

definition: it is a set with two binary operations and there are several axioms that these operations must satisfy

quotient

(有理数) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Both addition and multiplication are commutative and associative, and both have identity elements (0 for addition and 1 for multiplication)

$x \longrightarrow -x$ (additive inverse)

$x \longrightarrow \frac{1}{x}$ (multiplicative inverse except 0)

It is the existence of these inverses that allows us to define subtraction and division: $x - y$ means $x + (-y)$ and x/y means $x \cdot (\frac{1}{y})$

That covers all the properties that addition and multiplication satisfy individually. However, a very general rule when defining mathematical structures is that if a definition split into parts, then the definition as a whole will not be interesting unless those parts interact

distributive law relates addition and multiplication in some way, and thereby gives fields their special character. This is the rule that tell us how to multiply out the brackets:

$x(y + z) = xy + xz$ for any three numbers x, y, and z.

3° Vector spaces

A vector space is a mathematical structure in which the notion of linear combination makes sense. The objects that belong to the vector space are usually called vectors, unless we are talking about a specific example and are thinking of them as concrete objects such as polynomials or solutions of a differential equation.

Slightly more formally,

a set V such that, given any two vectors v and w (that is, elements of V) and

no space here

two real numbers a and b, we can form the linear combination $av + bw$

2 kinds of objects: the vectors v, w

the numbers a, b scalars from $\mathbb{F}$: V is a vector space over $\mathbb{F}$

4° Rings

not quite as central to mathematics as groups, fields, or vector spaces. roughly speaking, a ring is an algebraic structure that has most, but no necessarily all, of the properties of a field. In particular, the requirements of the multiplicative is less strict. The most important relaxation is that nonzero elements of a ring are not required to have multiplicative inverses; but sometimes multiplication is not even required to be commutative. If it is, then the ring itself is said to be commutative — a typical example of a commutative ring is the set $\mathbb{Z}$ of all integers. Another is the set of all polynomials with coefficients in some field $\mathbb{F}$.

Refer to ZJJ's notes:

definition: 设 A 和 K 是两个集合，定义

(1) 映射 $A \times A \to A$ 称为 A 上的内运算

(2) 映射 $K \times A \to A$ 称为 A 上的外运算

内运算和外运算都称为代数运算

由集合与满足一定运算规律的一些代数运算在一起组成的系统称为代数系统，或者把这样的系统称为具有代数结构的系统。

最常见的代数系统有以下三种类型：

① $\{X, \cdot\}$ 类型，$\cdot$ 为内运算；半群和群属于此类型

② $\{X, +, \cdot\}$ 类型，$+$ 和 $\cdot$ 为两个内运算；环，域，格，布尔代数都属于此类型。

③ $\{X, K, o\}$ 类型，o 为 X 上的外运算，即 X, K 又各有自己的内运算，线性空间属于此类

1. 群：

① 满足结合率的代数系统 $\{X, \cdot\}$ 称为半群

② 有单位元且每个元素都有逆元的半群称为群

③ 满足交换律的群称为交换群，或 Abel 群

例：E 为全集偶数集合，$+$ 为数的加法，$\times$ 为数的乘法，则 $\{E, \times\}$ 为半群

$\{E, +\}$ 为 Abel 群

4 axioms：

$\forall a, b \quad a \cdot b = c \in G$ (c: unique) [each element is unique]

① 封闭性 ② 结合律 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

③ 单位元 $e \cdot a = a \cdot e = a$

④ 逆元 $a^{-1} a = a \cdot a^{-1} = e$

2. 环：

定义：集合 X 上有两个内运算 $+$ 和 $\cdot$，若满足

① $\{X, +\}$ 为交换群

② $\{X, \cdot\}$ 为半群

③ 运算 $\cdot$ 对 $+$ 满足分配律

则称此 $\{X, +, \cdot\}$ 为环

若环的运算 $\cdot$ 也满足交换率，则称为交换环

将上述定义具体写出来即为

(a) $\forall\ a, b, c \in R$，$a+(b+c)=(a+b)+c$

$+$ 的结合律

(b) 至少有一个元素 $0 \in R$，使得 $0+a=a+0=a$

对所有 $a \in R$ 成立　　$+$ 的单位元

(c) 对任一 $a \in R$，存在 $-a \in R$，使得

$a+(-a)=(-a)+a=0$　　$+$：$a, -a$ 互逆

(d) 对所有 $a, b \in R$, $a+b=b+a$ + 交换

(e) 对所有 $a, b, c \in R$, $a\cdot(b\cdot c)=(a\cdot b)\cdot c$

· 结合律

(f) 对所有 $a, b, c \in R$, $a\cdot(b+c)=a\cdot b+a\cdot c$

且 $(a+b)\cdot c=a\cdot c+b\cdot c$

· 对 + 的分配律

当方便，称内运算 + 为加法，· 为乘法，则环有如下性质：

① 加法的单位元（记为 0）也是乘法的零元

$a+0=0+a=a \Rightarrow (a\cdot a)=(a+0)\cdot a$

$=a\cdot a+0\cdot a \Rightarrow 0\cdot a=0$

习惯上称乘法的零元为环的零元

乘法的单位元（如果存在）称为环的单位元

② 每个元素 x 关于加法的逆元记为 $-x$，则有恒等式 $(-a)\cdot b=a\cdot(-b)=-(a\cdot b)$

$$a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0$$

$$\Rightarrow (-a) \cdot b = -(a \cdot b)$$

例：在数的加法和乘法定义下，全体整数集是交换环，全体多项式的集合也是交换环

全体 $n \times n$ 矩阵的集合也是环，但不是交换环

注：在环的乘法里，没有对有任元和逆元提出要求。