1 几个主要研究对象

二元代数运算：一般的，非空集合S与自己的笛卡尔乘积$S \times S$到S的一个映射，称为S上的一个二元代数运算。

群：G被称为一个*群(group)*，如果G是一个非空集合，G上定义了一个a与b的二元代数运算，通常称为乘法，记作ab，适合下列条件：

(i)（结合律）对于G中的任意元素a, b, c，有$(ab)c = a(bc)$.

(ii)G中有一个元素e，使得$ea = ae = a, \quad \forall a \in G$.

e：群G的*单位元(identity element)*.

(iii)对于G中的任一元素a，都有G中的元素b，使得$ab = ba = e$.

b：群G中a的*逆元(inverse)*，b是唯一的，也记作a^{-1}. $\quad aa^{-1} = a^{-1}a = e$.

如果群G的运算满足交换律，即$ab = ba$，则称G为*交换群*（*abel group*）.

环：R被称为一个*环(ring)*，如果R是一个非空集合，R上定义了两个二元代数运算，通常称为加法和乘法，记作$a + b$和ab，适合下列条件：

(i)R对于加法成一个交换群.

(ii)（乘法的结合律）对于R中的任意元素a, b, c，有

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

(iii)（乘法对加法的分配律）对于R中的任意元素a, b, c，有

$$a(b + c) = ab + ac$$
$$(a + b)c = ac + bc$$.

如果环R对于乘法运算满足交换律，即$ab = ba$，则称G为*交换环(commutative ring)*.

如果环R中有元素e使得$ae = ea = a$，则称e是R的*单位元*，称R是有单位元的环（含幺环），通常把R的关于乘法运算单位元e记为**1**.（R关于加法运算的单位元是**0**）.在有单位元的环R中，对于元素a，如果有R中的元素b使得$ab = ba = 1$则称a为*可逆元(invertible element)*或*单位(unit)*，此时b称为a的逆元，记作a^{-1}，逆元是唯一的.

域：F被称为一个*域(field)*，如果F是一个有单位元$1(\neq 0)$的交换环，并且它的每一个非零元都可逆.域F有两个代数运算：加法和乘法，F关于加法构成**Abel**群，F的所有非零元组成的集合F^*关于乘法也构成**Abel**群，并且适合乘法对于加法的分配律.

有理数域Q，实数域R，复数域C都是域，当p为素数时，模p的剩余类环Z_p也是一个域，称为模p的剩余类域，一个域中若只有有限个元素，则称它为*有限域(finite field)*或*Galois域(galois field)*.

格：设$b_1, b_2, \cdots b_n$是R^m中的n个线性无关的向量$(m \leq n)$，**Z**为整数集，称$L(b_1, b_2, \cdots b_n) = \{\sum\limits_{i=1}^{n} x_i b_i : x_i \in Z\}$称为$R^m$中的一个格***(lattice)***，简记为**L**，并称$b_1, b_2, \cdots b_n$为格**L**的一组基，m为格**L**的维数，n为格**L**的秩.当$m = n$时，称格**L**是满秩的.

格的矩阵形式：格**L**的基也常写为矩阵的形式，即以$b_1, b_2, \cdots b_n$为列向量构成的矩阵$B = [b_1, b_2, \cdots b_n] \in Z^{m \times n}$，此时格**L**可以写作$L(B) = \{Bx : x \in Z^n\}$，定义格的行列式$det(L) = \sqrt{B^T B}$，与格基的选择无关，当格式满秩的时候格的行列式为矩阵**B**的行列式的绝对值即$det(L) = |det(B)|$.

像群，环，域，格这样具有代数运算的集合被称为代数结构***(algebraic structure)***.代数的主要研究对象是代数结构和保持运算的映射(称为态射***(morphism)***).