代数系统由集合和其上的运算组成，

本节首先介绍运算的概念和规律，

然后介绍讨论代数系统之间关系的工具：同构和同态，

定义 4.1 设 A 是一个非空集合，

我们称笛卡儿积 $A\times A$ 到 A 的映射φ为 A 上的一个二元运算，简称为运算，

一般地，若φ是 A 上的运算，且(a,b)在φ下的像为 c，则记 $a\varphi b=c$，

在不引起混淆的情况下，也可将 $a\varphi b$ 简记为 $a\bullet b$ 或 ab，

显然，集合的运算φ满足封闭性，即若 a 和 b 属于 A，则 $a\varphi b$ 属于 A，

另外，运算的像具有唯一性，即 $a\varphi b$ 是唯一确定的，

例 4.1 对属于 Z_n 的任意$\bar{a}$，$\bar{b}$，令$\bar{a}\varphi_1\bar{b}=\overline{ab}$，$\bar{a}\varphi_2\bar{b}=\overline{a+b}$，

试证明φ_1和φ_2均是 Z_n 上的运算，

证: 要说明φ_1是 Z_n 上的运算，

只需指出$\varphi_1: Z_n\times Z_n\to Z_n, (\bar{a},\bar{b})\to\overline{ab}$是一个映射即可

而这由例 1.5 可知，再由例 1.6 我们知道，φ_2也是 Z_n 上的运算，

φ_1和φ_2分别称为 Z_n(剩余类)上的乘法运算和加法运算，

并记$\bar{a}\varphi_1\bar{b}$为$\bar{a}\bullet\bar{b}$或$\overline{ab}$，而$\bar{a}\varphi_2\bar{b}$记为$\overline{a+b}$，

例 4.2 我们在集合 $M_n(R)$上定义运算 $\varphi: M_n(R)\times M_n(R)\to M_n(R), (A,B)\to AB$，

其中 $A\varphi B=AB$ 是 $M_n(R)$中通常的矩阵乘法，

则易知通常的矩阵乘法是 $M_n(R)$上的运算，

类似地，通常的矩阵加法也是 $M_n(R)$上的运算，

例 4.3 设非空集合 A 上所有变换构成的集合为 $T(A)=\{f|f:A\to A\}$，

若令 $\varphi:T(A)\times T(A)\to T(A),(\tau_1,\tau_2)\to\tau_1\tau_2$，

这里的 $\tau_1\varphi\tau_2=\tau_1\tau_2$ 就是 $T(A)$ 中通常的变换合成，则易知它是 $T(A)$ 上的运算，

一般地，我们称其为变换的乘法运算

设 φ 是集合 A 上的运算，A_0 是 A 的子集合，

若对属于 A_0 的任意 a，b，有 $a\varphi b$ 属于 A_0（φ 在 A_0 上封闭），

则 A_0 上有运算 $A_0\times A_0\to A_0,(a,b)\to a\varphi b$，这个运算仍用 φ 记，

即若集合的运算在子集合上封闭，则该运算也是子集合上的运算，

例 4.4 设 $H=\{\overline{0},\overline{3}\}$ 是 Z_6 的子集合，

则 Z_6 上的加法运算和乘法运算分别是 H 上的加法运算和乘法运算

因为 $\overline{0}+\overline{0}=\overline{0}$ 属于 H，$\overline{0}+\overline{3}=\overline{3}$ 属于 H，$\overline{3}+\overline{3}=\overline{0}$ 属于 H，

所以，Z_6 上的加法运算是 H 上的加法运算，

而 $\overline{0}\bullet\overline{0}=\overline{0}$ 属于 H，$\overline{0}\bullet\overline{3}=\overline{0}$ 属于 H，$\overline{3}\bullet\overline{3}=\overline{3}$ 属于 H，

因此，Z_6 上的乘法运算也是 H 上的乘法运算，

例 4.5 证明 Z_p 上的乘法运算也是 Z_p^* 上的乘法运算，这里 p 是素数，$Z_p^*=Z_p-\{\overline{0}\}$

证： 对属于 Z_p^* 的任意 $\overline{a}$，$\overline{b}$，有 $\overline{ab}\neq\overline{0}$，即 $\overline{ab}$ 属于 Z_p^*

所以 Z_p 上的乘法运算也是 Z_p^* 上的乘法运算，

注意，Z_p 上的加法运算不是 Z_p^* 上的加法运算（因为 $\overline{1}+\overline{p-1}=\overline{0}$ 不属于 Z_p^*），

例 4.6 设 $GL_n(R)$表示 $M_n(R)$中所有可逆矩阵构成的集合 ，

$SL_n(R)$表示 $M_n(R)$中所有行列式为 1 的矩阵构成的集合 ，

因为可逆矩库的乘积还是可逆矩阵 ，因此通常的矩阵乘法是 $CL_n(R)$上的运算

因为两个可逆矩阵的和不一定是可逆矩阵 ，

所以通常的矩阵加法不是 $CL_n(R)$上的运算 ，

类似地 ，我们知道矩阵的乘法运算是 $SL_n(R)$上的运算 ，

矩阵的加法运算不是 $SL_n(R)$上的运算

例 4.7 设 A 是一个非空集合 ，

则在 A 上的所有双变换构成的集合 S_A 上有乘法运算(变换的合成)，

若 $A=\{1,2,\cdots,n\}$，则 S_A 就是 n 元置换集合 S_n，

因为两个 n 元置换的合成(乘积)还是 n 元置换 ，所以 S_n 上有乘法运算 ，

偶置换的集合 A_n 是 S_n 的子集合 ，且两个偶置换的合成(乘积)还是偶置换 ，

所以 S_n 上的乘法运算也是 A_n 上的乘法运算 ，

若在两个集合上都有运算 ，则可以在这两个集合的笛卡儿积上构造一个运算

例 4.8 若设φ_1是集合 A_1 上的运算 ，φ_2是集合 A_2 上的运算 ，则容易验证

$(a_1,a_2)(b_1,b_2)=(a_1\varphi_1 b_1, a_2\varphi_2 b_2)$是 $A_1\times A_2$ 上的一个运算 ，

其中 a_i, b_i 属于 A_i，$i=1,2$，

定义 4.2 设 A 是一个非空集合 ，φ是 A 上的运算 ，若将 A 和φ作为一个整体 ，

则称 A 是(具有一个运算的)代数系统 ，记为$\{A;\varphi\}$，

若 A 有两个运算φ_1和φ_2 ，且我们把 A，φ_1和φ_2作为整体 ，

则称 A 是(具有两个运算的)代数系统 ，记为$\{A;\ \varphi_1\ ,\ \varphi_2\}$，

我们还可以把代数系统的概念向有多个运算的情形进行推广 ，

例 4.9$\{Z;+\}$，$\{R;\bullet\}$，$\{Z_n;+\}$，$\{M_n(R);+\}$，$\{GL_n(R);\bullet\}$，$\{SL_n(R);\bullet\}$，$\{S_n;\bullet\}$

和$\{A_n;\bullet\}$都是代数系统 ，

同样地 ，$\{Z;+,\bullet\}$，$\{R;+,\bullet\}$，$\{Z_n;+,\bullet\}$和$\{M_n(R);+,\bullet\}$也都是代数系统 ，

实际上，我们研究的代数系统，都被赋予了一定的条件，

一般来说，代数系统$\{A;\varphi\}$满足的条件可以分为两个方面：

一是集合 A 满足的条件，一是运算φ满足的条件，

例如，我们可以要求集合 A 满足有序性、度量性、拓扑性等等，

而要求运算φ满足结合律、交换律、分配律等等，

定义 4.3 设$\{A;\varphi\}$是代数系统，

如果对属于 A 的任意 a，b，c，有$(ab)c=a(bc)$，则称运算φ满足结合律，

如果对属于 A 的任意 a，b，有 $ab=ba$，则称运算φ满足交换律

定义 4.4 设$\{A;\varphi,\tau\}$是代数系统，

如果对属于 A 的任意 a，b，c，

有 $a\varphi(b\tau c)=(a\varphi b)\tau(a\varphi c)$(左分配律)和$(b\tau c)\varphi a=(b\varphi a)\tau(c\varphi a)$(右分配律)，

则称运算φ对τ满足分配律

注意，并不是所有的运算都能满足结合律，

即若$\{A;\varphi\}$是代数系统，则对于 A 中任意三个元素 a，b，c 来说，

(ab)c 和 a(bc)的运算结果可能不同，

例如，通常的整数减法运算“–”就不满足结合律

$(3–2)–1=1–1=0$，$3–(2–1)=3–1=2$，

但是，如果运算φ满足结合律，即$(ab)c=a(bc)$，

那么我们就可以将(ab)c 和 a(bc)简写为 abc，

当然，对于 A 中任意 n 个元素 $a_1,a_2,\cdots,a_n$，

我们可以将 $a_1(a_2(a_3\cdots))$记为 $a_1a_2\cdots a_n$，

特别地，当 $a_1=a_2=\cdots=a_n=a$ 时，我们记 $aa\cdots a=a^n$，

而且，$a^na^m=a^{n+m}$，$(a^n)^m=a^{nm}$，

例 4.10 易知，代数系统$\{Z;+,\bullet\}$的加法运算和乘法运算都满足交换律和结合律
并且乘法运算对加法运算满足分配律，
代数系统$\{Z_n;+,\bullet\}$的加法运算和乘法运算都满足交换律和结合律，
并且乘法运算对加法运算满足分配律，
代数系统$\{M_n(R);+,\bullet\}$的加法运算和乘法运算都满足结合律，
且乘法运算对加法运算满足分配律，
而加法运算满足交换律，但是乘法运算不满足交换律，
S_n和A_n的乘法运算满足结合律，
实际上，由代数系统的定义，我们很容易在一个集合上附加一个运算，
所以代数系统有无穷多个，
因此如何识别一个代数系统，
如何区分两个代数系统的异同就成了我们必须面对的问题

定义 4.5 设$\{A;\phi\}$和$\{A';\phi'\}$是两个代数系统，
如果 f 是 A 到 A'的双射，
且对属于 A 的任意 a，b，有$f(a\phi b)=f(a)\phi' f(b)$(保持运算)，
那么称 f 是$\{A;\phi\}$到$\{A';\phi'\}$的同构映射，
简称 f 是 A 到 A'的同构映射，或称 A 与 A'同构，记为$A\cong A'$，
类似地，若令$\{A;\phi,\psi\}$和$\{A';\phi',\psi'\}$是两个代数系统，
并且存在 A 到 A'的双射 f，满足对属于 A 的任意 a，b，
有$f(a\phi b)=f(a)\phi' f(b)$，$f(a\psi b)=f(a)\psi' f(b)$，
则称 f 是$\{A;\phi,\psi\}$到$\{A';\phi'\psi',\}$的同构映射，
简称 f 是 A 到 A'的同构映射，或称 A 与 A'同构，并记为$A\cong A'$，
更一般地，设$\{A;\phi_i\}_{i\in I}$和$\left\{A';\phi_i'\right\}_{i\in I}$是两个代数系统族，
如果 f 是 A 到 A'的双射且对属于 A 的任意 a，b，对属于 I 的任意 i，
有$f(a\phi_i b)=f(a)\phi_i' f(b)$(保持运算)，
那么称 f 是$\{A;\phi_i\}_{i\in I}$到$\left\{A';\phi_i'\right\}_{i\in I}$的同构映射，
注意，代数系统同构需要两个条件：双射和保持运算，

例 4.11 设 2Z 是偶数集合，则$\varphi: a \to 2a$ 是 Z 到 2Z 的双射

且$\varphi(a+b)=2(a+b)=2a+2b=\varphi(a)+\varphi(b)$，其中 a，b 属于 Z，

所以，φ是$\{Z; +\}$到$\{2Z; +\}$的同构映射，$Z \cong 2Z$，

例 4.12 集合$H=\{0, 1, -1\}$关于整数的乘法运算构成一个代数系统，

但该代数系统与$\{Z_3; +\}$不同构，

因为若这两个代数系统之间存在同构映射$\varphi: Z_3 \to H$，

则$\varphi(\overline{0})=\varphi(\overline{1}+\overline{2})=\varphi(\overline{1})\varphi(\overline{2})$，

又因为φ是双射，这就要求在 H 中有两个不同元素的乘积等于第三个元素，

但在 H 中任意两个不同元素的乘积都不等于第三个元素，因此φ不存在，

命题 4.1 设 f 是$\{A; \phi, \psi\}$到$\{A'; \phi', \psi'\}$的同构映射，则

(1)ϕ(或ψ)满足结合律⇔ ϕ'(或ψ')满足结合律，

(2)ϕ(或，ψ)满足交换律⇔ ϕ'(或ψ')满足交换律，

(3)ψ对ϕ满足分配律⇔ ψ'对ϕ'满足分配律

证: 这里仅给出(2)的证明，

设ϕ满足交换律，对属于 A 的任意 a'，b'，

因为 f 是满射，所以存在属于 A 的 a，b，使得 f(a)=a'，f(b)=b'，

又因 f 是 A 到 A'的同构映射(保持运算)，

所以 a'ϕ'b'=f(a)ϕ'f(b)=f(aϕb)=f(bϕa)=f(b)ϕ'f(a)=b'ϕ'a'，

即ϕ'满足交换律

反之，设ϕ'满足交换律，

对属于 A 的任意 a，b，有 f(aϕb)=f(a)ϕ'f(b)=f(b)ϕ'f(a)=f(bϕa)，

又因为 f 是单射，所以 aϕb=bϕa，即ϕ满足交换律

实际上，若两个代数系统同构，

尽管表面上看来集合和运算不尽相同，但它们体现的性质相同，

我们把在同构映射下保持不变的代数系统的性质统称为代数性质，

即两个同构的代数系统的代数性质相同，

一个代数系统的所有代数性质统称为这个代数系统的代数结构，

研究代数系统的首要目的，就是确定所有互不同构的代数系统的代数性质，

但是，构造代数系统间的双射往往是比较困难的，

因此，我们常常在运算条件保持不变的前提下，

将映射的条件放宽，利用同态比较两个代数系统，

定义 4.6 设$\{A;\phi\}$和$\{A';\phi'\}$是两个代数系统，

如果 f 是 A 到 A'的映射且对属于 A 的任意 a，b 有 $f(a\phi b)=f(a)\phi' f(b)$，

那么称 f 是$\{A;\phi\}$到$\{A';\phi'\}$的同态映射，

简称 f 是 A 到 A'的同态映射，或称 A 与 A'同态，记为 $A\sim A'$，

特别地，若 f 是$\{A;\phi\}$到$\{A';\phi'\}$的同态，且 f 是单(或满)射，

则称 f 是 A 到 A'的单(或满)同态，

类似地，可以定义具有多个代数运算的代数系统之间的同态、单同态和满同态，

例 4.13 设$\phi: Z\to Z_n$，$a\to\bar{a}$，则ϕ是 Z 到 Z_n 的满射，

且对属于 Z 的任意 a，b，

有$\phi(a+b)=\overline{a+b}=\bar{a}+\bar{b}=\phi(a)+\phi(b)$，$\phi(ab)=\overline{ab}=\bar{a}\,\bar{b}=\phi(a)\phi(b)$，

因此，ϕ是$\{Z;+,\bullet\}$到$\{Z_n;+,\bullet\}$的满同态，

例 4.14 设 $\det: GL_n(R)\to R^*\quad A\to\det(A)$，

其中 R^*表示去掉 0 后的实数的子集合，

则容易验证行列式映射 det 是代数系统$\{CL_n(R);\bullet\}$到$\{R^*;\bullet\}$的满同态，

命题 4.2 设 f 是{A ; ϕ , ψ}到{A' ; ϕ' , ψ'}的满同态 ，

则(1)ϕ(或ψ)满足结合律⇒ϕ'(或ψ')满足结合律 ，

(2)ϕ(或ψ)满足交换律⇒ϕ'(或ψ')满足交换律 ，

(3)ψ对ϕ满足分配律⇒ψ'对ϕ’满足分配律 ，