代数笔记整理

文嘉明

2019 年 10 月 26 日

目录

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$ea = ae = a$， $\forall a \in G$.

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}. $aa^{-1} = a^{-1}a = e$.

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$L(b_1, b_2, \cdots b_n) = \{\sum_{i=1}^{n} x_i b_i : x_i \in Z\}$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)***).

2 群

2.1 群的定义

群：一个群是指一个非空集合G满足下列四个条件：
(i) 在G上定义的一个二元代数运算.
(ii) G上的运算适合结合律.
(iii) G中有一个元素e，使得$ea = ae = a$， $\forall$**a**$\in G$.
(iv)G中的每一个元素都有逆元.
如果G满足条件(i)(ii)，则称G为*半群(semigroup)*，如果G满足条件(i)(ii)(iii)，则称G为*幺半群(monoid)*.

在群G中：
$a^{-1} = b^{-1}$则$a = (a^{-1})^{-1} = (b^{-1})^{-1} = b$(这里用到用到逆元的唯一性).
$(ab)^{-1} = b^{-1}a^{-1}$，进而有$(a_1a_2\ldots a_n)^{-1} = a_n^{-1}\ldots a_1^{-1}$.

元素的方幂：对于正整数n，n个a的乘积记作a^n，我们规定$a^0 = e$，$a^{-n} = (a^{-1})^n$.

有限群：若一个群有有限个元素，则称它为*有限群(finite group)*，元素的个数称为群G的*阶(order)*，记作$|G|$.

循环群：如果群G的每一个元素都能写成G中某一个元素a的倍元（对于群的运算），则称G为*循环群(cyclic group)*，把a叫做群G的*生成元(generator)*，此时可以把群G记作$\langle a\rangle$.

例如，整数加群Z是一个无限循环群，n次单位根群U_n是一个阶为n的有限循环群，循环群都是Abel群.

域F上所有n阶可逆矩阵组成的集合，对于矩阵乘法构成一个群，称为域F上的一个n阶*一般线性群(general linear group)*，记作$GL_n(F)$.域F上所有行列式为1的n阶可逆矩阵，对于矩阵乘法也构成域F上的n阶*特殊线性群(special linear group)*，记作$SL_n(F)$.实数域上所有n阶正交矩阵，对于矩阵乘法构成n阶*正交群*O_n*(orthogonal group)*，实数域上所有行列式为1的n阶正交矩阵，对于矩阵乘法构成n阶*特殊正交群*SO_n*(special orthogonal group)*.

2.2 子群,陪集,Lagrange定理,循环群

子群：群G的非空子集H如果对于G的运算也成一个群，则称H为G的*子群(subgroup)*，记作**H≤G**.例如$SO_n \le SL_n(R) \le GL_n(R)$ 和$SO_n \le O_n \le GL_n(R)$.

平凡子群：群G本身和仅由单位元素$\{e\}$构成的子群是G的两个*平凡子群(trivial subgroups)*.

由定义可知，若H是G的子群，则有
(1)$a, b \in H \Rightarrow ab \in H$.
(2)H与G有相同的单位元e.
(3)$a \in H \Rightarrow a^{-1} \in H$.

子群的判定方法：设H是G的非空子集，如果H满足：“$a, b \in H \Rightarrow ab^{-1} \in H$”，则$H$是$G$的子群.

证明：由于H非空，则H中至少存在一个元素a，由已知条件$aa^{-1} \in H$，即$e \in H$.对$\forall b \in H$，有$b^{-1} = eb^{-1} \in H$.任取$c, b \in H$，有$b^{-1} \in H$，因此$cb = c(b^{-1})^{-1} \in H$，这表示$G$的运算也是$H$的运算，且由于$H$是$G$的子集运算的结合律是成立的，由子群的定义，$H$是$G$的子群.

等价关系：对于集合**G**上的一个二元关系“$\sim$”，如果它有(1)自反性,即$a \sim a$;(2)对称性,即$a \sim b$则$b \sim a$;(3)传递性,即$a \sim b, b \sim c$则$a \sim c$，则称“$\sim$”为一个*等价关系(equivalence relation)*.

群G和它的一个子群H，利用H定义一个二元关系如下：对于$a, b \in G$，规定$a \sim b \Leftrightarrow b^{-1}a \in H$，容易验证，“$\sim$”是一个等价关系，利用等价关系“$\sim$”对$G$进行划分. 对于$a \in G$，等价类$\bar{a}$=$\{x \in G \mid x \sim a\} = \{x \in G \mid a^{-1}x \in H\} = \{x \in G \mid a^{-1}x = h, h \in H\} = \{x \in G \mid x = ah, h \in H\} = \{ah \mid h \in H\}$.

左陪集：$aH = \bar{a} = \{ah \mid h \in H\}$，称$aH$为群$G$的一个*左陪集(left coset)*，并称$a$为左陪集$aH$的一个代表，子群$H$的本身是一个左陪集($H = eH$)，易有$aH = bH \Longleftrightarrow b^{-1}a \in H$，子群$H$的两个陪集或者相等，或者不相交.

左商集：群G中，由子群H的所有左陪集组成的集合称为G关于H的*左商集(left quotient set)*，记作$(G/H)_l$.

类似的可以定义Ha和$(G/H)_r$ ，称为群G的*右陪集(right coset)*和*右商集(right quotient set)*.

定义如下一个映射，构建左商集与右商集的关系：

$$f : (G/H)_l \to (G/H)_r$$

$$aH \longmapsto Ha^{-1}$$

由于$aH = bH \Longleftrightarrow b^{-1}a \in H \Longleftrightarrow (b^{-1})(a^{-1})^{-1} \in H \Longleftrightarrow Hb^{-1} = Ha^{-1}$结合陪集的性质，可以得到$f$是一个单射，而$f$显然是一个满射，故$f$为双射.即左商集$(G/H)_l$和右商集$(G/H)_r$之间存在一一对应，群$G$关于子群$H$的左商集（或右商集）的基数称为$H$在$G$中的*指数(index)*,记作$[G : H]$.如果群$G$的子群$H$在$G$中的指数$[G : H] = r$，则$H$的所有左陪集可组成$G$的一个划分，$G = H \sqcup a_1H \sqcup a_2H \sqcup \ldots \sqcup a_{r-1}H$.(“$\sqcup$”代表不交并)

Lagrange定理：有限群G的任一子群H的阶必为群G的阶的因子，更精确的，我们有$|G| = |H|[G:H]$

由**Lagrange**定理可以得到素数阶(**p**阶)群G中的任何一个元素a，a的阶为**p**的因数，从而a不是单位元时，a的阶只能为**p**，从而$G = \langle a \rangle$，即素数阶群一定为循环群.根据这一结论，可以给出**Fermat**小定理的一个简短证明.

Fermat小定理(Fermat's little theorem)：如果**p**是素数，并且a不是**p**的倍数，则 $a^{p-1} \equiv 1(modp)$.

证明：由于a不是**p**的倍数，因此$\bar{a} \in \mathbf{Z}_p^+$，由于$|Z_p^+|$=**p-1**，故$|a| = p-1$，即$a^{p-1} \equiv 1(modp)$.

下面给出两个常用的循环群的结论：
(**1**)循环群的每一个子群都是循环群.
(**2**)对于**n**阶循环群$G = \langle a \rangle$，任给$a^k \in G$，$0 \le k \le n-1$，循环子群$H = \langle a^k \rangle$的阶为$\frac{n}{(n,k)}$.
(**3**)对于循环群G的阶**n**的每一个正因子**s**，都存在唯一的**s**阶子群，它们组成G的全部子群.

证明：
(**1**)设H是循环群$G = \langle a \rangle$的非平凡子群，则H中有G的非单位元，由于H是一个有限群，故存在幂指数最小的元，记作$a^k(k \ne 0)$，对于$\forall a^n \in H$，设$q = lk + r$ﬁ$0 \le r < k$，则$a^r = a^{q-lk} = a^q(a^k)^{-l} \in H$，$r \ne 0$时与$a^k$的取法矛盾，因此$r = 0$，$a^q = (a^k)^l \subseteq \langle a^k \rangle$，于是$H \subseteq \langle a^k \rangle$，$H = \langle a^k \rangle$.

(**2**)设$|a^k|$=**s**，设$n = n_1(n,k), k = k_1(n,k)$，其中$(n_1,k_1) = 1$，由于$(a^k)^{n_1} = a^{k_1(n,k)n_1} = a^{k_1 n} = e$，因此$a^k$的阶$s|n_1$，由于$e = (a^k)^s = a^{ks}$，因此$n|ks$.即$n_1(n,k)|k_1(n,k)s$，从而$n_1|k_1 s$，由于$(n_1,k_1) = 1$，因此$\mathbf{n}_1$|**s**，综上所述，$s = n_1 = \frac{n}{(n,k)}$

(**3**)设**s**是G的阶**n**的任一正因子，则存在正整数d，使得$n = ds$.$|a^d| = \frac{n}{(n,d)} = \frac{n}{d} = s$，因此$\langle a^d \rangle$是$G$的一个**s**阶子群.下证唯一性：设$H$是$G$的任意一个**s**阶子群，则由(**1**)可以知道H是一个循环群，设$H = \langle a^k \rangle$，$|a^k| = s = \frac{n}{d}$，又$|a^k| = s = \frac{n}{(n,k)}$，因此$(n,k) = d$.存在$u,v \in Z$使得$un + vk = d$.于是$a^d = a^{un+vk} = a^{un}a^{vk} = (a^k)^v \in \langle a^k \rangle$，从而$\langle a^d \rangle \subseteq \langle a^k \rangle$，又它们的阶均等于s，因此$\langle a^d \rangle = \langle a^k \rangle = H$，这也就证明了$G$的s阶子群唯一.

2.3 群的同构与直积,群的同态,正规子群

群的同构：设G和G'是两个群，如果存在G到G'的一个双射σ，使得对于G中任意两个元素a,b，都有$\sigma(ab)=\sigma(a)\sigma(b)$.那么称$G$与$G$ß是同构的*(isomorphic)*，记作$G\cong G'$，称$\sigma$是$G$到$G'$的一个同构映射，简称为同构*(isomorphism)*.

同构的性质：
(1)任意一个无限循环群都与Z同构，任意一个m阶循环群都与Z_m同构.
(2)σ把G的单位元e映成G'的单位元e'.
(3)对于任意$a\in G$，σ把G中a的逆元a^{-1}映成G'中$\sigma(a)$的逆元$\sigma(a)^{-1}$，即$\sigma(a^{-1})$=$\sigma(a)^{-1}$.
(4)对于任意$a\in G$，a与$\sigma(a)$的阶相同.
(5)G的子群H在σ下的像$\sigma(H)$是G'的子群.

前面已经证明了素数阶群一定是循环群，因此2阶群、3阶群、5阶群、7阶群等都是循环群，从而2阶群恰有一个同构类，3阶群、5阶群、7阶群也都是类似的，自然会问：4阶群有多少个同构类呢？

Z_4是一个4阶循环群.K=$\{$(1),(12)(34),(13)(24),(14)(23)$\}$是一个4阶群，但K中所有非单位元都是2阶元，K没有4阶元，因此K与Z_4不同构，从而4阶群至少有两个同构类，下证K只有这两个同构类.

证明：设G为4阶群，若G有4阶元a，则$G=\langle a\rangle$，$G\cong Z_4$.

下面考虑G没有4阶元的情形，则G的3个非单位元a,b,c都是2阶元.又$ab\neq e$(否则结合b是2阶元，有$b=b^{-1}=a$与$a\neq b$矛盾)且$ab\neq a,b$，从而$ab=c$同理可以得到$ba=c$，故$ab=ba=c,ac=ca=b,bc=cb=a$，此时有$G\cong K$.

综上所述，4阶群有两个同构类：一类是四阶循环群，它的代表是Z_4，另一类是4阶非循环的Abel群，它的代表可以取K.有没有更简单的4阶非循环的Abel群代表呢？

群的直积：考虑Z_2×Z_2=$\{(\bar{0},\bar{0})(\bar{0},\bar{1}),(\bar{1},\bar{0}),(\bar{1},\bar{1})\}$，规定$(a_1,a_2)+(b_1,b_2)=(a_1+b_1,a_2+b_2)$，其中$a_i,b_i\in Z_2$.构成一个以$(\bar{0},\bar{0})$为单位元的Abel群，易于验证$(\bar{0},\bar{1}),(\bar{1},\bar{0}),(\bar{1},\bar{1})$都是2阶元，因而$Z_2$×$Z_2$与K同构.像这样，群G和G'是两个群，在它们的笛卡尔积$G\times G'$上定义一个二元运算$(g_1,g_1')(g_2,g_2')=(g_1g_2,g_1'g_2')$，显然这个运算满足结合律，有单位元$(e,e')$，$(g,g')$有逆元$(g^{-1},g'^{-1})$，因此$G\times G'$构成一个群，称它为群$G$与$G'$的直积*(direct product)*，记作$G$×$G'$.如果群$G$和$G'$的运算都记成加法，则直积$G$×$G'$的运算也记成加法，此时可以称直积$G$×$G'$是群$G$与$G'$的直和*(direct sum)*，记作$G\oplus G'$.

直和的性质：
(1)如果群G和群G'都是有限群，则$G\times G'$是有限群，$|G\times G'|$=$|G||G'|$.如果G或G'是无限群，则$G\times G'$是无限群.
(2)如果群G和群G'都是Abel群，则$G\times G'$是Abel群.
(3)$G\times G'$与$G'\times G$同构，同构映射可以取$(g,g')\longmapsto(g',g)$.
(4)两个以上的群的直积也可以类似的定义.

Z_m×Z_n是循环群当且仅当$(m,n)=1$.即Z_m×Z_n=Z_{mn}当且仅当$(m,n)=1$.

群的同态：设G和G'是两个群，如果存在G到G'的一个映射σ，使得对于G中任意两个元素a, b，都有$\sigma(ab) = \sigma(a)\sigma(b)$.则称$\sigma$是$G$到$G'$的一个同态映射，简称为同态*(homomorphism)*.(比起“同构”，少了σ是双射.)

同态的性质：
(1)σ把G的单位元e映成G'的单位元e'.
(2)对于任意$a \in G$，σ把G中a的逆元a^{-1}映成G'中$\sigma(a)$的逆元$\sigma(a)^{-1}$，即$\sigma(a^{-1}) = \sigma(a)^{-1}$.
(3)G的子群H在σ下的像$\sigma(H)$是G'的子群.
(4)G在σ下的像$Im\sigma$是G'的子群，称$Im\sigma$为同态σ的像*(image)*.

同态的核：设σ是群G到群G'的一个同态，则G'的单位元e'的原像集称为σ的核*(Kernel)*，记作$Ker\sigma$，$Ker\sigma = \{a \in G | \sigma(a) = e'\}$.由定义易知$Ker\sigma$是$G$的一个子群.

单同态与满同态：设σ是群G到群G'的一个同态，如果σ是满射，则称σ是满同态*(surjective homomorphism)*，如果σ是单射，则称σ是单同态*(injective homomorphism)*或嵌入*(embedding)*.σ是满同态当且仅当$Im\sigma{=}G'$，σ是单同态当且仅当$Ker\sigma = \{e\}$.

核的性质：设σ是群G到G'的一个同态，记$K = Ker\sigma$，则$gKg^{-1} = K, \forall g \in G.$

证明：对于任意给定的$g \in G$，任取$x \in K$，有$\sigma(gxg^{-1}) = \sigma(g)\sigma(x)\sigma(g^{-1}) = \sigma(g)e'\sigma(g)^{-1} = e'$.因此$gxg^{-1} \in K$，从而$gKg^{-1} \subseteq K$.对任意$y \in K$，有$y = g(g^{-1}yg)g^{-1} \in gKg^{-1}$，于是$KKg^{-1}$.综上所述，$gKg^{-1} = K, \forall g \in G$.

正规子群：由上面这个例子启发，抽象出下述重要概念，群G的一个子群N，如果满足$gNg^{-1} = N, \forall g \in G$,则称$N$是$G$的一个正规子群*(normal subgroup)*，记作$N \triangleleft G$.例如σ是群G到G'的一个同态时，$Ker\sigma \triangleleft G$.$e$和$G$本身都是$G$的平凡的正规子群，$G$的其余正规子群(如果有的话)都是非平凡的.

共轭子群：容易验证，群G的一个子群H，对任意的$g \in G$如果满足gHg^{-1}也是G的一个子群，称H是G的一个共轭子群*(conjugate subgroup)*，群G的一个子群N是G的正规子群当且仅当N的所有共轭子群都是N本身.

正规子群的判定：群G的一个子群H是G的正规子群当且仅当对于G的每一个元素a，都有$aH = Ha.$

证明：必要性：$H \triangleleft G$，则对$\forall a \in G$，有$aHa^{-1} = H$，于是对于任意的$h \in H$有$aha^{-1} \in H$，从而$ah = (aha^{-1})a \in Ha$，得到了$aH \subseteq Ha$，类似可以证明$Ha \subseteq aH$，进而得到$aH = Ha$.

充分性：对$\forall g \in G$，任取$H \in H$，由题设可知$gH = Hg$，因此存在$h' \in H$使得$gh = h'g$，从而$ghg^{-1} = h' \in H$，即$gHg^{-1} \in H$，类似的有$g^{-1}Hg \in H$，故对$\forall y \in H$有$y = g(g^{-1}Hg)g^{-1} \in gHg^{-1}$，即$H \in gHg^{-1}$，综上所述$gHg^{-1} = H \forall g \in G$，即$H \triangleleft G$.

证明正规子群的方法：由充分性的证明可以归纳出证明正规子群的方法，设H是G的一个子群，如果对于任意给定的$g \in G$，任取$h \in H$，都有$gHg^{-1} \in H$，则H是G的正规子群.且有
(1)Abel群的每一个子群都是正规子群.
(2)如果H是G的指数为2的子群，则H是G的正规子群.(由$G = H \cup aH = H \cup Ha$得到$aH = Ha$)

现在开始利用正规子群研究群的结构，设G是N的一个正规子群，则对$\forall a\in G$，有$aN=Na$，从而$(G/H)_l=(G/H)_r$，G关于正规子群N的左右商集形成了统一，称为G关于N的商集***(quotient set)***，记作G/N.任取正规子群N的两个左陪集aN,bN，有$(aN)(bN)=a(Nb)N=a(bN)N=(abN)N=ab(NN)=abN$(注意集合的乘法$AB=\{ab\in A,b\in B\}$)，在商集$G/N$上定义二元运算$(aN)(bN)=abN$，易于验证$G/N$构成一个群，称为$G$对于正规子群$N$的商群***(quotient groups)***.当G是有限群时，$N\lhd G$，商群G/N的阶等于$\frac{|G|}{|N|}$.

设N是群G的一个正规子群，令

$$\pi:G\to G/N$$

$$a\longmapsto aN,$$

则π是群G到商群G/N的一个满同态，且$Ker\pi=N$.称π为自然同态***(natural homomorphism)***.商群是群G在自然同态下的像，正规子群N是自然同态的核而由之前的结论有群G到G'的任一同态σ的核$Ker\sigma$是G的正规子群，可以得到如下的群同态基本定理.

群同态基本定理：设σ是群G到G'的一个同态，则同态像同构于商群$G/Ker\sigma$，即$G/Ker\sigma\cong\mathbf{Im}\sigma$.

证明：记$N=Ker\sigma$，则$N\lhd G$，从而有商群G/N，作映射φ

$$\varphi:G/N\to Im\sigma$$

$$aN\longmapsto\sigma(a),$$

由于$aN=bN\Longleftrightarrow b^{-1}a\in N\Longleftrightarrow\sigma(b^{-1}a)=e'\Longleftrightarrow\sigma(a)=\sigma(b)$，因此$\varphi$是$G/N$到$Im\sigma$的一个单射，显然$\varphi$是满射.对于任意$aN,bN\in G/N$,有$\varphi((aN)(bN))=\varphi(abN)=\sigma(ab)=\sigma(a)\sigma(b)=\varphi(aN)\varphi(bN)$，因此$\varphi$是$G/N$到$Im\sigma$的一个同构，从而$G/Ker\sigma\cong Im\sigma$.

可以给出例子：群Z到群Z_m有一个满同态σ，且$Ker\sigma=mZ$，根据群同态基本定理得：$Z/mZ\cong Z_m$

第一同构定理：设G是群，$H\leq G,N\lhd G$，则**(1)**$HN\leq G$**(2)**$H\cap N\lhd H$，且$H/H\cap N\cong HN/N$.

第二同构定理：设G是群，$H\lhd G$，$N\lhd G$，且$N\subseteq H$，则$H/N\lhd G/N$且$(G/N)/(H/N)\cong G/H$.

群同态基本定理反映了群G的每一个同态像都同构于G对于同态核的商群，又同态核是G的正规子群，因此掌握了群G的所有正规子群，就掌握了G的所有同态像，从而可以了解群G的结构，反之亦然.这就是正规子群在研究群的结构中起着十分重要的作用的缘故.

单群：如果一个群G只有平凡的正规子群，则称G为单群***(simple group)***.单群没有非平凡的正规子群，因此单群的同态像或者同构于$\{\mathbf{e}\}$，或者同构于G自身.通俗的说，单群抱成一团，无法把它拆开，单群之于群论就像素数之于整数理论，**Abel**群G是单群当且仅当G是素数阶循环群.

2.4 Z_n^*和椭圆曲线上的有限群

这一节重点结合密码学中的应用，介绍两个具体的有限交换群的例子：Z_n^*和椭圆曲线上的有限交换群.

Z_n^*：Z_n^*表示模p的既约剩余系的集合，任意$\bar{a},\bar{b}\in Z_n^*$，定义乘法：$\bar{a}\times\bar{b}=\overline{a\times b}$，则($Z_n^*$,×)构成一个交换乘群且$Z_n^*$的阶为$\varphi(n)$.(欧拉函数$\varphi(n)$表示不超过n的与n互素的数的个数)

证明：先证明(Z_n^*,×)是一个群：如果$\bar{a}=\bar{a'},\bar{b}=\bar{b'}$，则$\mathbf{n}|a-a',n|b-b'$，所以$\mathbf{n}|(a-a')\times b+(b-b')\times a'=a\times b-a'\times b'$，即$\overline{a\times b}=\overline{a'\times b'}$，这表明了“×”是一个二元运算. Z_n^*对“×”满足封闭和结合律，且$\bar{1}$为单位元，对每个$\bar{a}\in Z_n^*$有逆元$\overline{a^{-1}}$，其中$aa^{-1}=1\pmod n$，且由$\bar{a}\times\bar{b}=\overline{a\times b}=\overline{b\times a}=\bar{b}\times\bar{a},\forall\bar{a},\bar{b}\in Z_n^*$可知交换律成立.因此，$(Z_n^*,\times)$的元素个数为$\varphi(n)$的有限交换群.

椭圆曲线：椭圆曲线*(Elliptic Curves)*E是由标准形式的三次曲线$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$(系数$a_i$属于数域$K$)，的所有解$(x,y)\in K^2$的集合，以及一个无穷远点$\mathcal{O}$组成.对于一般的域$K$，如果$a_2\neq 0$，则椭圆曲线可以表示成$y^2=x^3+ax+b$.在椭圆曲线$E$上定义加法“+”：设$P(x_1,y_1),Q(x_2,y_2)\in E$，$\mathcal{O}$是椭圆曲线上的无穷远点，则

(1)$P+\mathcal{O}=P$.

(2)若$x_1=x_2,y_1=-y_2$，则$P+Q=\mathcal{O}$

(3)其他情形，$P+Q=(x_3,y_3)$，其中$x_3=\lambda^2-x_1-x_2,y_3=\lambda(x_1-x_3)-y_1$. $\lambda=\begin{cases}\frac{y_2-y_1}{x_2-x_1}(P\neq Q)\\ \frac{3x_1^2+a}{2y_1}\ (P=Q)\end{cases}$

$nP=\underbrace{P+P+\cdots+P}_{n}$，$0P=\mathcal{O}$

椭圆曲线的几何意义：

当$x_1\neq x_2$时，P与Q的连线与椭圆曲线相交于点$R=(x_3,y_3)$，那么$P+Q+R=\mathcal{O}$.

当$x_1=x_2,y_1=y_2$时，作P点处的切线与椭圆曲线的另一交点R满足$P+P+R=\mathcal{O}$，R关于x轴的对称点即为$2P$.

当$x_1=x_2,y_1=-y_2$时，P与Q的连线与x轴垂直，与椭圆曲线交于无穷远点$\mathcal{O}$，故$P+Q=\mathcal{O}$.

莫代尔定理(Mordell-Weil thoerem)：椭圆曲线上的有理点集合G关于加法构成有限交换群.

证明：用到代数数论的方法，此处暂时略去.

2.5 群上的离散对数问题

离散对数：设G是循环群，g是它的一个生成元.群G中的离散对数问题是指：给定G中的一个元素h，找到正整数**n**，使得$h = g^n$，我们把**n**叫做h(相对于生成元g)的离散对数，记作$n = \log_g n$

显然我们可以通过将h和所有的$g^t, 1 \leq t < |G|$进行比较的方法来求解G中的离散对数问题，这种方法称为蛮力求解或者穷举搜索，最多需要$|G|$次G中的运算，因此对阶数较大的群是不实用的.某些循环群中的离散对数问题被认为是难以求解的，但是从技术上讲，由于阶数相同的循环群都是同构的，因此，离散对数问题的困难性不是依赖于群本身，而是依赖于群的表示.

例**1**：考察整数在加法运算下构成的群$(Z, +)$，则**1**是**Z**的一个生成元，因此**Z**中的离散问题就是，任给$h \in Z$，求**n**使得$n \cdot 1 = h$，这是一个平凡的问题.

例**2**：设**n**是一个正整数，Z_n是模**n**的剩余类组成的加法群，$\alpha \in Z_n$是Z_n的一个生成元.那么Z_n中的离散对数问题就是给定的$\beta \in Z_n$，求解x使得$x\alpha = b \pmod n$，因为α是Z_n的一个生成元有$gcd(\alpha, n) = 1$，所以α有模**n**的乘法逆元α^{-1}，利用欧几里得算法将它求出可以得到$\log_\alpha \beta = x = \beta\alpha^{-1}$

假设G是一个阶为**n**的有限阶循环群，α是G的一个生成元，φ是G和Z_n之间的一个同构映射，则可以得到$\varphi(xy) = \varphi(x)\varphi(y) \pmod n \Rightarrow \varphi(\alpha^x) = x\varphi(\alpha) \pmod n$，所以$\beta = \alpha^x \Leftrightarrow \varphi(\beta) = x\varphi(\alpha) \pmod n$，这样利用和例**2**类似的方法求解$x$，可以得到$\log_\alpha \beta = \varphi(\beta)(\varphi(\alpha))^{-1} \pmod n$

由上面的例子可以看出，如果我们能够找到有效的方法找出G和Z_n之间的同构映射，那么我们就能有有效的方法计算G中的离散对数问题.反过来，若有计算G中的离散对数问题的有效算法，也容易构造出G和Z_n之间的同构映射.但问题是，有时我们虽然知道G和Z_n是同构的，但我们并没有有效的算法来清楚的刻画这种结构.离散对数问题的困难型经常被用来设计密码学原子构建，目前人们比较感兴趣的两类离散对数问题分别是有限域中的离散对数问题和有限域上的椭圆曲线中的离散对数问题.

3 环与域

3.1 环与域的定义,子环

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.

零因子：环R中的一个元素a称为一个*左（或右）零因子(left(right)zero divisor)*，如果R中有元素$b\neq 0$，使得$ab=0$(或$ba=0$).左零因子和右零因子都简称为零因子，**0**是平凡的零因子，其余的零因子是非平凡的，若R没有非平凡的零因子，则称R为*无零因子环* .

整环：有单位元$1(\neq 0)$的无零因子的交换环称为*整环(integral domain)*.

除环：如果环R的所有非零元组成的集合R^*对于乘法构成一个群，即R是有单位元的环且每个非零元都可逆，则R称为*除环(division ring)*.

域：交换的除环称为*域(field)*，即F被称为一个域，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/galois field)*.

子环：如果环R的一个非空子集R_1对于R的加法和乘法也成为一个环，则称R_1是R的一个*子环(subring)*.环R的一个非空子集R_1是子环的充要条件是：R_1对于R的减法和乘法都封闭，即$a,b\in R_1\Rightarrow a-b, ab\in R_1$.

3.2 环的理想,商环,环的同态与同构

理想：设R是一个环，I是R的一个非空子集.如果I对于减法封闭，即$a \in I, b \in I \Rightarrow a - b \in I$.且$I$具有“吸收性”，即$a \in I, r \in R \Rightarrow ar \in I, ra \in I$.则称$I$为$R$的一个*理想(ideal)*或者*双边理想*.如果I对于减法封闭，并且具有“左(或右)吸收性”，即$a \in I, r \in R \Rightarrow ar \in I$(或$ra \in I$)则称$I$为$R$的一个*左(或右)理想(left(right)ideal)*.

由于理想对减法封闭，所以I是R的加法群的子群.理想是从代数几何中代数簇的研究里抽象得到的代数结构.

单环：显然**0**和R是环R的理想，称为平凡的理想，如果环R只有平凡的理想，则称R为*单环(simple ring)*.

在整数环Z中，一个整数**m**的所有倍数组成的集合mZ是Z的一个理想.在域F的一元多项式环$F[x]$中，一个多项式$f(x)$的所有倍式组成的集合是$F[x]$的一个理想.一般地，设R是一个含幺交换环，$a \in R$，把集合$\{ra | r \in R\}$记作Ra，容易看出Ra是R的一个理想，一列理想I_j的交集$\cap I_j$也是一个理想.

生成的理想和主理想：设S是环R的一个非空子集，环R的包含S的所有理想的交称为*由S生成的理想(ideal generated by S)*，记作(S)，如果$S = \{a_1, a_2, \cdots, a_n\}$，则称$(S)$是*有限生成的*，并把$(S)$记作$(a_1, a_2, \cdots, a_n)$.由一个元素$a$生成的理想称作*主理想(principal ideal)*，记作(a).

R是有单位元的交换环，则Ra是由一个元素a生成的理想，因此Ra是主理想，Ra可以记作(a)，特别地，在整数环Z中mZ是主理想，可记作(m).

理想的和与积：若A, B是R的两个非空子集，易验证，如果I, J都是R的理想，则$I + J, IJ$也是R的理想，且有$IJ \subseteq I \cap J \subseteq I + J$.(其中$A + B = \{a + b | a \in A, b \in B\}$，$AB = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n | a_i \in A, b_i \in B\}$)

理想的互素：在整数环Z中，m, n是整数，$(m, n) = 1$时$(m) + (n) = (1) = Z$，由此抽象出互素的概念：R是有单位元的环，I, J是R的理想，如果$I + J = R$，则称I与J*互素(coprime)*.

互素的性质：
(1)设R是由单位元的交换环，I, J是R的理想，I与J互素，则$IJ = I \cap J$.
(2)设R是由单位元的交换环，I, J, K是R的理想，如果I和J都与K互素，则IJ与K互素.

商环：设R是一个环，I是R的一个理想，则I是R的加法群的子群.由于R的加法群是一个**Abel**群，因此I是正规子群，从而有商群R/I，它的元素是陪集$r + I$，定义$(r_1 + I)(r_2 + I) = (r_1r_2 + I)$，可以验证这个乘法是定义良好的，且满足结合律和左右分配律，因此R/I是一个环，称为R对于I的*商环(quotient ring)*，商环R/I中的元素$r + I$称为模I的*剩余类(residue class)*.

商环的性质：
(1)如果环R有单位元**1**，则商环R/I有单位元**1+I**.
(2)如果环R是交换环，则商环R/I也是交换环.

环的同态：设R和R'是两个环，如果存在R到R'的一个映射σ，使得对于R中任意两个元素a, b，满足$\sigma(a + b) = \sigma(a) + \sigma(b)$,$\sigma(ab) = \sigma(a)\sigma(b)$.则称$\sigma$是$R$到$R'$的一个*同态映射*，简称为*同态(homomorphism)*.(若环R, R'有单位元$1, 1'$，还要求$\sigma(1) = 1'$).

同态的性质：
(1)σ把R的单位元e映成R'的单位元e'.
(2)对于任意$a \in R$，σ把G中a的逆元a^{-1}映成R'中$\sigma(a)$的逆元$\sigma(a)^{-1}$，即$\sigma(a^{-1})$=$\sigma(a)^{-1}$.
(3)R的加法子群H在σ下的像$\sigma(H)$是R'的加法子群.
(4)R在σ下的像$Im\sigma$是R'的子群，称$Im\sigma$为同态σ的像*(image)*.$Im\sigma$不仅是R'的加法群的子群，而且是环R'的一个子环.

同态的核：设σ是环R到环R'的一个同态，则R'的单位元e'的原像集称为σ的核***(Kernel)***，记作$Ker\sigma$，$Ker\sigma = \{a \in G | \sigma(a) = e'\}$.由定义易知$Ker\sigma$是环$R$的加法群一个子群，也是环$R$的一个理想.

单同态与满同态：设σ是环R到环R'的一个同态，如果σ是满射，则称σ是满同态*(surjective homomorphism)*，如果σ是单射，则称σ是单同态*(injective homomorphism)*或嵌入*(embedding)*.σ是满同态当且仅当$Im\sigma = R'$，σ是单同态当且仅当$Ker\sigma = \{e\}$

设I是环R的一个理想，令

$$\pi : R \to R/I$$

$$r \longmapsto r + I,$$

则π是环R到商环R/I的一个满同态，保持加法和乘法运算.如果环R有单位元1则$\pi(1) = 1 + I$，且$Ker\pi = I$.称π为自然同态*(natural homomorphism)*.商环是环R在自然同态下的像，理想I是自然同态的核$Ker\pi$.

环同态基本定理：设σ是群G到G'的一个同态，则同态像同构于商环$R/Ker\sigma$，即$R/Ker\sigma \cong Im\sigma$.

证明：由于σ也是环**R**的加法群到**R'**的加法群的一个同态，因此根据群同态基本定理得$R/Ker\sigma$与$\mathbf{Im}\sigma$同构，它的一个同构映射为

$$\varphi : R/Ker\sigma \to Im\sigma$$

$$r + Ker\sigma \longmapsto \sigma(r),$$

只需证明φ保持乘法：$\varphi(r_1 + Ker\sigma)(r_2 + Ker\sigma) = \varphi(r_1r_2 + Ker\sigma) = \sigma(r_1r_2) = \sigma(r_1)\sigma(r_2) = \varphi(r_1 + Ker\sigma)\varphi(r_2 + Ker\sigma)$.因此$\varphi$是$R/Ker\sigma$到$Im\sigma$的一个同构映射，从而$R/Ker\sigma$与$Im\sigma$的同构.

环的同构：若同态σ是双射，则称R与R'是同构的*(isomorphic)*，记作$R \cong R'$，σ是R到R'的一个同构映射，简称为同构*(isomorphism)*.

类似于群的第一、第二同构定理，有环的第一、第二同构定理如下：

第一同构定理：设R是群，H是R的子环，I是R的理想，则(1)$I + H$是R的子环(2)$I \cap H$是H的理想，且有环同构$H/I \cap H \cong I + H/I$.

第二同构定理：设R是环，I, J都是R的理想，且$I \subseteq J$，则J/I是R/I的理想，且有环同构$(R/I)/(J/I) \cong R/J$.

环同态基本定理反映了环R的每一个同态像都同构于R对于同态核的商群，又同态核是R的理想，因此掌握了群R的所有理想，就掌握了R的所有同态像，从而可以了解环R的结构，反之亦然.这就是理想在研究环的结构中起着十分重要的作用的缘故.

3.3 素理想与极大理想,环的直和

在上一节中我们已经定义了理想的互素：R是有单位元的环，I, J是R的理想，如果$I+J=R$，则称I与J互素.这是根据Z中的互素满足$(m,n)=1$时$(m)+(n)=Z$，抽象得到的互素的概念.类似的抽象出根据整数环可以抽象出如下定义：

素理想：若R的一个理想$P \neq R$，使得对任意的$a,b \in R, ab \in P \Rightarrow a \in P$或$b \in P$，则称$P$为$R$的一个***素理想(prime ideal)***.

极大理想：若R的一个理想$M \neq R$，使得对任意的理想$I \subseteq R$，若$M \subseteq I$，则$I=M$或$I=R$，则称M为R的一个***极大理想(maximal ideal)***.

设R是一个有单位元的交换环，$P \subseteq R$是R的一个理想，则P是R的素理想当且仅当R/P是整环.

设R是一个有单位元的交换环，$M \subseteq R$是R的一个理想，则M是R的极大理想当且仅当R/M是域.(极大理想的定义是由域的性质引出，由域都是整环，可以得到极大理想一定是素理想，反之不成立，如$Z[x]/(x)$是整环但不是域，从而(x)是$Z[x]$的一个素理想，但不是极大理想.)

谱：设R是含单位元$1(\neq 0)$的交换环，则R的所有素理想组成的集合称为R的***谱(spectrum)***，简称为$SpecR$.

环的直和：设$R_1, R_2, \cdots, R_n$都是环，作$R_1, R_2, \cdots, R_n$加法群的直和$R_1 \bigoplus R_2 \bigoplus \cdots \bigoplus R_n$，定义乘法如下：$(a_1, a_2, \cdots, a_n) \cdot (b_1, b_2, \cdots, b_n) = (a_1b_1, a_2b_2, \cdots, a_nb_n)$，这个乘法满足结合律和左右分配律，因此$R_1 \bigoplus R_2 \bigoplus \cdots \bigoplus R_n$是一个环，称为$R_1, R_2, \cdots, R_n$的直和.它的零元是$(0,0,\cdots,0)$，如果每个环都有单位元$1_i$，它的单位元是$(1_1, 1_2, \cdots, 1_n)$，如果每个环都是交换环，则$R_1 \bigoplus R_2 \bigoplus \cdots \bigoplus R_n$也是交换环.

同余：设I是环R的一个理想，对于$a,b \in R$，如果$a-b \in I$，则称a,b模***I同余(a is congruent to b modulo I)***，记作$a = b \pmod{I}$.同余关系具有反身性，对称性和传递性，因此是一个等价关系.容易看出a的等价类$\bar{a}=a+I$从而R对于模I同余的商集就是商环R/I.

引理：设R是有单位元$1(\neq 0)$的环，它的理想$I_1, I_2, \cdots, I_s$两两互素，则$R/I_1 \cap I_2 \cap \cdots \cap I_s \cong R/I_1 \bigoplus R/I_2 \bigoplus \cdots \bigoplus R/I_s$.
证明：构建映射

$$\sigma : R \to R/I_1 \cap I_2 \cap \cdots \cap I_s$$

$$x \longmapsto (x+I_1, x+I_2, \cdots, x+I_s),$$

验证σ是环R到环$R/I_1 \bigoplus R/I_2 \bigoplus \cdots \bigoplus R/I_s$的一个同态，结合环同态基本定理可以得到$R/I_1 \cap I_2 \cap \cdots \cap I_s \cong Im\sigma$.由$I_s$两两互素证明$\sigma$是满射，从而原结论成立.

中国剩余定理：设**R**是有单位元$1(\neq 0)$的环，理想$I_1, I_2, \cdots, I_s$两两互素，则对于任意的**s**个元素$b_1, b_2, \cdots b_s \in R$，同余方程组$x = b_j \pmod{I}_j (\forall j = 1, 2, \cdots s)$在$R$内必有解，且如果**a,c**为两个解，则$a = c \pmod{I_1 \cap I_2 \cap \cdots \cap I_s}$.(由$\sigma$是满射可以得到该同余方程组有解，由同余关系的对称性和传递性可得到解在模**I**意义下唯一)

推论：设R是有单位元$1(\neq 0)$的环，它的理想$I_1, I_2, \cdots, I_s$两两互素，且$I_1 \cap I_2 \cap \cdots \cap I_s = (0)$，则有$R \cong R/I_1 \bigoplus R/I_2 \bigoplus \cdots \bigoplus R/I_s$.

3.4 唯一分解整环,主理想整环,Euclid整环

我们已经知道，整数环**Z**的结构：每一个正整数可以唯一地分解成有限多个素数的乘积(不考虑排列顺序)，域F上的一元多项式环$F[x]$的结构：每一个次数大于0的多项式都可以分解成有限多个不可约多项式的乘积，且在相伴意义下分解唯一.**Z**和$F[x]$都是整环，自然地，将这个结论抽象到一般的整环中.

因子与倍元：设R是一个整环，对于任意取定的$a, b \in R$，如果存在$c \in R$，使得$a = bc$，则称b整除a，记作$b|a$，此时称b是a的*因子(factor/divisor)*，a是b的*倍元(multiple)*.整除关系具有反身性和传递性，没有对称性但有相伴性见下文.

u是R的单位(即可逆元)当且仅当$u|1$，即$(u) = R$，R单位u是R的每一个元素a的因子，因为$a = u(u^{-1}a)$.

相伴：$b|a \Leftrightarrow (b) \supseteq (a)$，如果$b|a, a|b$则称$a$与$b$*相伴(associate)*，记作$a \sim b$，相伴是一个等价关系.$a \sim b \Leftrightarrow (a) = (b) \Leftrightarrow R$的单位$u$使得$a = bu$.

真因子与平凡因子：如果$b|a$但$a \not| b$(即b是a的因子但b不是a的相伴元)，则称b是a的*真因子(proper factor)*.不难看出，若u是单位则u没有真因子.对R中的给定元素a，R的所有单位和a的任一相伴元都称为a的*平凡因子(trivial factor)*，a的其他因子(如果还有的话)称为a的非平凡因子.

可约：设$a \in R$，$a \neq 0$，且a不是单位，若a只有平凡因子，则称a是*不可约的(irreducible)*，否则称a是*可约的(reducible)*.

素元：设$a \in R$，$a \neq 0$，且a不是单位，如果从$a|bc$可以推出$a|b$或$a|c$，则称a是一个*素元(prime element)*

在整环R中，素元一定是不可约元，反之不成立.(如整环$Z[\sqrt{-5}]$中3和$2 \pm \sqrt{-5}$都是不可约元，但都不是素元)

在整环R中，a为素元当且仅当(a)为非零素理想.由此可以得到如果元素a生成的理想(a)为非零极大理想，则a为素元，进而a为不可约元.

最大公因子：设$a, b \in R$，如果存在$c \in R$，使得$c|a, c|b$，则称c是a和b的*公因子(common divisor)*.a, b的一个公因子d被称为*最大公因子(greatest common divisor)*，如果$c|a, c|b$可以推出$c|d$，d也记作$gcd(a, b)$.

引理：在整环R中，如果每一对元素都有最大公因子，则对任意$a, b, c \in R$，有$(ca, cb) \sim c(a, b)$.

唯一分解整环：整环R满足下列两个条件,：
(1)R中的每一个非零且非单位的元素a可以分解成有限多个不可约元的乘积:$a = p_1 p_2 \cdots p_s$;
(2)上述分解在相伴意义下是唯一的，即如果a有两个分解式$a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_l$，则$t = s$，并且可以将$q_j$的下标适当改写可使得$p_i \sim q_i, i = 1, 2, \cdots s$.
则称R是一个*唯一因子分解整环(unique factorization domain)*或*Gauss整环(Gauss domain)*

下面探讨怎样的整环是唯一分解整环，首先研究唯一分解整环的性质.

唯一分解整环的性质：

(1)设R是唯一因子分解整环，则

(1)R的每一对元素都有最大公因子;

(2)R的每一个不可约元都是素元;

(3)因子链条件***(divisor chain condition)***成立，即如果$a_1, a_2, a_3, \cdots$中，每一个a_i都是a_{i-1}的真因子，则这个序列是有限序列.

唯一因子分解整环的判定：整环R如果满足下列两个条件，则R是唯一因子分解整环：

(1)因子链条件;

(2)每一个不可约都是素元.(可换为"每一对元素都有最大公因子".因为由**(2)**可以推出R的每一个不可约元都是素元)

主理想整环：整数环**Z**和一元多项式环$F[x]$的每一个理想都是主理想，由此抽象出主理想整环的概念.一个整环R称为***主理想整环(principal ideal domain)***，如果R的每个理想都是主理想，记作PID.

主理想整环的性质：

(1)主理想整环中不可约元**p**生成的理想(**p**)一定是极大理想.则R是唯一因子分解整环.

(2)主理想整环一定是唯一因子分解整环.

Euclid整环：整数环**Z**和一元多项式环**F[x]**都有带余除法，由此抽象出**Euclid**整环的概念.一个整环**R**称为***Euclid整环(Euclidean domain)***，如果存在R^*到自然数集N的一个映射δ，使得对任意$a, b \in R$且$b \neq 0$，都有$h, r \in R$满足$a = hb + r, r = 0$或$r \neq 0$且$\delta(r) < \delta(b)$.

Euclid整环都是主理想整环.

4 格

4.1 格的定义

设**R**是实数集，R^m是**m**维欧式空间，在R^m上定义了内积$< x, y >= x^T y$，以及向量长度$\|x\| = \sqrt{x^T x}$.

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$L(b_1, b_2, \cdots b_n) = \{\sum_{i=1}^{n} x_i b_i : x_i \in Z\}$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$det(L) = |det(B)|$.

Gram-Schmidt正交化：与线性代数类似，可以对R^m中的格**L**的一组基(一组线性无关的向量)$b_1, b_2, \cdots b_n$进行**Gram-Schmidt**正交化，规定$b_1^* = b_1, b_i^* = b_i - \sum_{i=1}^{i-1} \mu_{i,j} b_j^*, i > 1$,其中$\mu_{i,j} = \frac{<b_i, b_j^*>}{<b_j^*, b_j^*>}, 1 \leq j < i \leq n$，得到$R^m$中的一组正交向量$b_1^*, b_2^*, \cdots b_n^*$，注意这里$b_1^*, b_2^*, \cdots b_n^*$通常不是格**L**的基.格**L**的行列式满足$det(L) = \prod_{i=1}^{n} b_i^*, det(L) \leq \prod_{i=1}^{n} b_i$.

格上的最短向量问题：格上的最短向量问题是指格中一个最短的非零向量的问题(**shortest vector problem,SVP**)，这一问题已被证明在随机约化下是**NP-**困难问题，我们首先考虑在一个给定的特殊区域里是否存在某个事先给定的格的非零向量问题.

Minkowski定理：设**L**是R^m中的格，**S**是R^m中的一个可测的关于原点对称的凸集$(\alpha\beta \in S \Rightarrow \alpha + \beta/2) \in S$，若**S**的体积$\mu(S) \geq 2^n f det(L)$，则$S \cap L$中有非零向量.（这个结论来自代数数论，在此处证明略去）

格的最短向量长度的上界：设**L**是R^m中秩为n的格,设格**L**中的最短向量的长度为λ_1，那么$\lambda_1 \leq \sqrt{n} det(L)^{\frac{1}{n}}$(在$span(b_1, b_2$取区域**S**为以原点为中心$\sqrt{n} det(L)^{\frac{1}{n}}$为半径的开球中，其中包含一个$n$维的边长为$2det(L)^{\frac{1}{n}}$的超立方体，体积满足**Minkowski**定理的条件，故在内部存在向量$v \in S \cap L$使得$\rfloor v \rfloor \leq \sqrt{n} det(L)^{\frac{1}{n}}$)

4.2 格基约化算法(LLL算法)

上一节中介绍了格中最短向量长度的一个上界，但没有构造出具体的短向量，本节我们介绍约化基的概念和用格基约化算法找出格中的短向量，为了叙述方便，本节中格**L**均指维数为n的满秩格.

5 有限域的结构

5.1 有限域的定义与构造,域扩张

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)*.

子域与扩域：设F是域，K是F的子集，如果K在F的运算下也构成一个域，则称K为F的*子域(subfield)*，F为K的*扩域(extension field)*或*域扩张(field extension)*，记作K/F，特别的如果$K\neq F$则称K为F的*真子域*，K的包含F的任一子域称为K/F的*中间域(intermediate field)*.

域的特征：设F是域，如果存在正整数**n**使得对任何$r\in R, n\cdot r=0$，但对于任何小于**n**的正整数$n', n'\cdot r\neq 0$，则称**n**为域F的特征，否则称域F的特征为**0**.域F的特征记作$char(F)$.

素域：一个域如果不包含任何真子域，则称为*素域*.如果一个域F的子域作为域是素域，则称该子域为F的*素子域*.任意多个子域的交仍然是子域，可以证明一个域的素子域实际上就是该域的所有子域的交.

有理数域**Q**和阶为素数**p**的**Galois**域F_p都是素域.一个域F的素子域在特征为**p**时同构于阶为**p**的**Galois**域F_p，在特征为**0**时同构于有理数域**Q**.

有限域的构造：由3.4我们已经知道，R是一个有单位元的交换环，$M\subseteq R$是R的一个理想，则M是R的极大理想当且仅当R/M是域.利用这条性质，我们可以从小的有限域出发构造大的有限域.

定理：设F_q是含有q个元素的有限域，其中$q=p^r, p$为素数.如果$m(x)=a_0+a_1x+\cdots+a_nx^n$是$F_q[x]$的**n**次不可约多项式，则$F_q[x]/(m(x))$是含有$q^n$个元素的有限域，并且它的每一个元素可以唯一地表示成$c_0+c_1x+\cdots+c_{n-1}x^{n-1}$，其中$c_i\in F_q, 0\leq i<n, u=x+(m(x)), u$满足$a_0+a_1u+\cdots+a_nu^n=0$.

证明：由于$m(x)$是$F_q[x]$的**n**次不可约多项式，因此$(m(x))$是$F_q[x]$的一个极大理想.根据上面的结论有$F_q[x]/(m(x))$是一个域，由$m(x)=a_0+a_1x+\cdots+a_nx^n$是$F_q[x]$的**n**次不可约多项式，$F_q[x]/(m(x))$中的元素形如$c_0+c_1x+\cdots+c_{n-1}x^{n-1}+(m(x))$，(由带余除法得到)，则由带余除法的过程知这种表示是唯一的，且$c_i\in F_q, 0\leq i<n$，因此每个c_i都有q种选取方式，从而$|F_q[x]/(m(x))|=q^n$，$F_q[x]/(m(x))$是一个含q^n个元素的有限域.

令$u=x+(m(x))$，作单同态$\sigma: F_q\to F_q[x]/(m(x)), a\longmapsto a+(m(x))$可以将$a$与$a+(m(x))$等同，从而有$c_0+c_1x+\cdots+c_{n-1}x^{n-1}+(m(x))=[c_0+(m(x))]+[c_1+(m(x))][x+(m(x))]+\cdots+[c_{n-1}+(m(x))][x+(m(x))]^{n-1}=c_0+c_1u+\cdots+c_{n-1}u^{n-1}$.因此$F_q[x]/(m(x))$中的元素可以唯一地表示成$c_0+c_1x+\cdots+c_{n-1}x^{n-1}$，其中$c_i\in F_q, 0\leq i<n, u=x+(m(x))$，因为$a_0+a_1u+\cdots a_nu^n=a_0+a_1x+\cdots a_nx^n+(m(x))=(m(x))$故在商环$F_q[x]/(m(x))$中有$a_0+a_1u+\cdots+a_nu^n=0$.

可以证明：有限域F的元素个数**q**一定是一个素数**p**的方幂，其中**p**是域F的特征.这个定理给出了从**q**元有限域F_q出发构造出q^n元有限域的方法：首先在$F_q[x]$中找到一个**n**次不可约多项式$m(x)$，然后作商环$F_q[x]/(m(x))$，即为一个q^n元的有限域，且每个元素可以唯一的表示，我们尝试将这样的方法推广到任何一个域F.

例如，对于实数域$\mathbf{R}$，在$\mathbf{R}[\mathbf{x}]$中取**2**次不可约多项式$m(x) = x^2+1$，作商环$R[x]/(x^2+1)$，则它是一个域且$R[x]/(x^2+1) = \{a+bu|a,b \in R\}$，其中$u = x+(x^2+1)$满足$u^2+1 = 0$，可以构建$R[x]/(x^2+1)$到$\mathbf{C}$ 的映射$\sigma, \sigma(a+bu) = a+bi$，容易验证$\sigma$是一个环同构.虽然R中不存在$\sqrt{-1}$，但是在域$R[x]/(x^2+1)$中有$u^2 = -1$从而$u = \sqrt{-1}$，这里将$-1$与$-1+(x^2+1)$等同.

域扩张：K是F的子域，M是F的任何子集.$K(M)$定义为F中所有含有M和K的子域的交，称为添加M中的元素得到的K的*扩域/扩张*.显然$K(M)$是含有K和M的最小的子域.当$M = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$时，我们记$K(M) = K(\alpha_1, \alpha_2, \alpha_n)$.特别地称$K(\alpha)$为*单扩域/单扩张*，$\alpha$称为$K(\alpha)$在$K$上的定义元，有$F(\alpha) = F[\alpha]$.

代数扩张：设K是域F的一个子域，$\alpha \in F$，如果α满足K上的一个非零多项式，则称α是K上的*代数元*，不是代数元的元素称为*超越元*.如果一个扩张K/F，K的每一个元素都是F上的代数元，则称域扩张K/F是*代数扩张(algebraic extension)*

有限扩张：设K/F是一个域扩张，则K可以看成是域F上的一个线性空间，它的加法运算是域K中的加法，它的纯量乘法运算是域F的元素与K的元素作K中的乘法运算.K作为域F上的线性空间的维数称为K在F上的*次数(degree of K over F)*，记作$[K:F]$.如果$[K:F]$是有限的，则称K是F上的*有限扩张(finite extension)*，此时K作为F上的线性空间的一个基也叫做域扩张K/F的一个*基(basis)*.

K/F是有限扩张，则K的每个元素都是F上的代数元.进而有限扩张一定是代数扩张.

K/F是域扩张，$\alpha \in K$且α是F上的代数元.如果α在F上的极小多项式$m(x)$的次数为**n**，则$[F(\alpha):F] = n$，且$1, \alpha, \alpha^2 \cdots \alpha^{n-1}$是$F(\alpha)/F$的一组基.

设有三个域$F \subseteq L \subseteq K$，则$[K:F]$有限当且仅当$[K:L]$和$[L:F]$都有限，此时有$[K:F] = [K:L][L:F]$.

分裂域：$f(x)$是域F上的一个$n(\geq 1)$次多项式，域扩张E/F称为$f(x)$在F上的一个*分裂域(splitting field)*，如果满足：
(1)$f(x)$在$E[x]$中完全分解成一次因式的乘积$f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n), \alpha_i \in E, 1 \leq i \leq n;$
(2)$E = F(\alpha_1, \alpha_2, \cdots \alpha_n)$.

设$f(x)$是域F上的多项式，$n = deg(f(x)) \geq 1$.那么$f(x)$的分裂域一定存在，且$[E:F] \leq n!$

5.2 有限域的特征性质