# 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$(a_1a_2 \dots a_n)^{-1} = a_n^{-1} \dots a_1^{-1}$.

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$SO_n \leq SL_n(R) \leq GL_n(R)$ 和$SO_n \leq O_n \leq GL_n(R)$.

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$a^k\in G$，$0\leq k\leq n-1$，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$a^k(k\neq 0)$，对于$\forall a^n\in H$，设$q=lk+r$fi$0\leq r<k$，则$a^r=a^{q-lk}=a^q(a^k)^{-l}\in H$，$r\neq 0$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$(a^k)^{n_1}=a^{k_1(n,k)n_1}=a^{k_1n}=e$，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$n_1|k_1s$，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$\sigma$，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)$\sigma$把$G$的单位元$e$映成$G'$的单位元$e'$.
(3)对于任意$a \in G$，$\sigma$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$\sigma$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$Z_2 \times Z_2$=$\{(\bar{0},\bar{0})(\bar{0},\bar{1}),(\bar{1},\bar{0}),(\bar{1},\bar{1})\}$，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$Z_2 \times Z_2$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$(g_1, g_1')(g_2, g_2') = (g_1 g_2, g_1' g_2')$，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$G \times G'$.如果群$G$和$G'$的运算都记成加法，则直积$G \times G'$的运算也记成加法，此时可以称直积$G \times G'$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.

$Z_m \times Z_n$是循环群当且仅当$(m, n) = 1$.即$Z_m \times Z_n$=$Z_{mn}$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$\sigma$，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$\sigma$是双射.)

同态的性质：
(1)$\sigma$把$G$的单位元$e$映成$G'$的单位元$e'$.
(2)对于任意$a\in G$，$\sigma$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$\sigma$下的像$\sigma(H)$是$G'$的子群.
(4)$G$在$\sigma$下的像$Im\sigma$是$G'$的子群，称$Im\sigma$为同态$\sigma$的像*(image)*.

同态的核：设$\sigma$是群$G$到群$G'$的一个同态，则$G'$的单位元$e'$的原像集称为$\sigma$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$\sigma$是群$G$到群$G'$的一个同态，如果$\sigma$是满射，则称$\sigma$是满同态*(surjective homomorphism)*，如果$\sigma$是单射，则称$\sigma$是单同态*(injective homomorphism)*或嵌入*(embedding)*.$\sigma$是满同态当且仅当$Im\sigma$=$G'$，$\sigma$是单同态当且仅当$Ker\sigma=\{e\}$.

核的性质：设$\sigma$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$N\lhd G$.例如$\sigma$是群$G$到$G'$的一个同态时，$Ker\sigma\lhd G$.$e$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：$H\lhd G$，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$H\lhd G$.

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$\pi$是群$G$到商群$G/N$的一个满同态，且$Ker\pi=N$.称$\pi$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$\sigma$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$\sigma$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$\varphi$

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

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

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$\sigma$，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，$H\le G,N\lhd G$，则**(1)**$HN\le G$**(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$\alpha$是$Z_n$的一个生成元有$gcd(\alpha, n) = 1$，所以$\alpha$有模**n**的乘法逆元$\alpha^{-1}$，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，$\alpha$是$G$的一个生成元，$\varphi$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.