9 椭圆曲线

椭圆曲线是算术代数几何中一类极为重要的曲线，它将朴素的数论与深刻的几何学结合到一起，在当今的数论研究中具有深远的影响。著名的费马大定理的证明，就是借助了椭圆曲线的知识。此外，有限域上椭圆曲线的离散对数计算等问题，构成了公钥密码学的一类主要问题，在信息科学中得到广泛的应用。

本章主要介绍椭圆曲线的相关内容，包括仿射和射影空间，代数曲线，椭圆曲线，椭圆曲线上的群结构，椭圆曲线上的离散对数等。

9.1 仿射空间与射影空间

本节介绍仿射空间与射影空间，讨论其相关性质，为下面进一步介绍椭圆曲线的定义与性质做预备。首先，我们先从熟悉的实数域 $\mathbf{R}$ 上二维平面出发，引入仿射、摄影平面与空间概念。在本节中，定义 F 为域，域 K 为域 F 的扩域或代数闭包。

例 9.1.1 我们先考虑实数域 $\mathbf{R}$ 上的二维平面 $\mathbf{R}^2$。

对于 $\mathbf{R}^2$ 任意非原点 $(a,b)\neq(0,0)$ 构成的集合：

$$\mathbf{R}^2\setminus(0,0)=\{(a,b)\mid a,b\in\mathbf{R},(a,b)\neq(0,0)\}。$$

我们建立其上的一种关系 $\sim$ ：

若在 $P_1=(a_1,b_1)$，$P_2=(a_2,b_2)$ 同一条过原点的直线上，则 $P_1\sim P_2$。

或者说，

$(a_1,b_1)\sim(a_2,b_2)$ 当且仅当存在 $\lambda\in\mathbf{R}\setminus\{0\}$ 使得 $a_1=\lambda a_2,b_1=\lambda b_2$

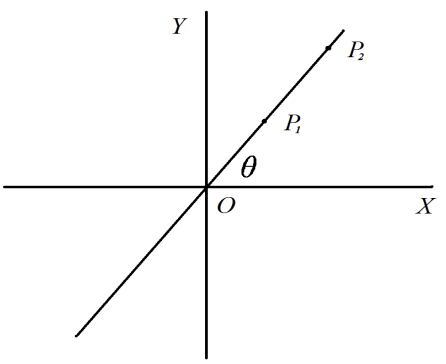

图 9.1.1

我们容易验证上述关系是等价关系。自然地，我们考虑由该等价关系导出的等价类：

$$\{\mathbf{R}^2 \setminus (0,0)\}/\sim$$

根据前面等价关系的定义，该等价类可以由过原点的直线唯一表示。也就是说，我们可以用过原点直线（相对横坐标轴）的斜率代表该直线，进而代表该等价类。具体地，若以$[x,y]$表示点(x,y)所在的等价类，我们有：

1）当$y\neq 0$时，对$[x,y]$，定义$[x,y]\mapsto \frac{x}{y}$，易验证该映射是一一映射。

2）当$y=0$时，依照定义有$x\neq 0$，对$[x,y]$，定义$[x,y]\mapsto \infty$，也可记$\frac{x}{0}=\infty$。

这样，我们就建立了$\{\mathbf{R}^2 \setminus (0,0)\}/\sim$与$\mathbf{R}\cup\{\infty\}$的一一映射。其中，$\infty$对应于横坐标轴，我们称之为集合$\{\mathbf{R}^2 \setminus (0,0)\}/\sim$中的无穷远点。

下面，我们将上述的定义从实数域上二维平面扩展到一般域上的 n 维空间。

定义 9.1.1a　给定域 K，我们称

$$\mathbf{A}^n(K)=\{P=(a_1,\cdots,a_n)\mid a_i\in K,1\le i\le n\}$$

为 ***K* 上的 *n* 维仿射空间**，也可简记为$\mathbf{A}^n$。其中的$P=(a_1,\cdots,a_n)$称为$\mathbf{A}^n$中的点，a_i称为P的坐标。此外，对于 K 的子域F，称$\mathbf{A}^n(F)=\{P=(a_1,\cdots,a_n)\mid a_i\in F,1\le i\le n\}$为$\mathbf{A}^n$ **的 F −有理点集**。

当然，对 n=2 的情形，我们简称集合 $K^2=\{(x,\ y)\mid x,\ y\in K\}$称为域 K 上的**仿射平面**。K^2中的元素称为仿射平面上的点, 可以用仿射坐标$(x,\ y)$表示. 例如中学里讲过的笛卡儿平面就是实数域$\mathbf{R}$上的仿射平面, 又称为欧氏平面.

在介绍了上述仿射空间概念后，我们给出射影空间的定义。

定义 9.1.1b 给定$\mathbf{A}_K^{n+1}\setminus\{0,\cdots,0\}$中的等价关系：

$$(a_0,\cdots,a_n)\sim(\lambda a_0,\cdots,\lambda a_n),\quad \lambda\in K^*$$

集合$\mathbf{A}_K^{n+1}\setminus\{0,\cdots,0\}$在上述等价关系下的等价类

$$\mathrm{P}_K^n=\{[a_0,\cdots,a_n]\mid a_i\in K,1\le i\le n+1,\text{且不同时为}0\},$$

称为域 ***K* 上的 *n* 维射影空间**，记作$\mathbf{P}_K^n$，或$\mathbf{P}^n$。其中$a_i\in K,1\le i\le n+1$称为$\mathbf{P}^n$的**齐次坐标**。

例 9.1.2 我们考虑$\mathbf{C}$上一维射影平面$\mathbf{P}_{\mathbf{C}}^1$，易知其由等价类由

$$(\{(x,y)\mid x,y\in\mathbf{C}\}\setminus(0,0))/\sim=\{[x,y]\mid x,y\in\mathbf{C},\text{且不同时为}0\}$$

构成。实际上，上述等价类可以由 $\mathbf{C}\cup\{\infty\}$ 确定：

1）当 $y\neq 0$ 时，对 $[x,y]$，有 $\frac{x}{y}\mapsto\mathbf{C}$，是一一映射。

2）当 $y=0$ 时，有 $x\neq 0$，对 $[x,y]$，记 $\frac{x}{y}=\infty$。该点对应于复直线上的无穷远点。

下面，我们介绍这两种空间中零点集、代数集的概念，从而建立第八，九章中多项式环与两类空间的联系。

定义 9.1.2a K 为代数闭域，设 $K[x_1,\cdots,x_n]$ 为 K 上的 n 元多项式环，$f(x_1,\cdots,x_n)$ 是 $K[x_1,\cdots,x_n]$ 中的一个多项式，我们称

$$Z(f)=\{P\in\mathbf{A}^n\mid f(P)=0\}$$

为 n 元多项式 f 的**零点集**。

类似地，T 是 $K[x_1,\cdots,x_n]$ 的子集，我们称

$$Z(T)=\{P\in\mathbf{A}^n\mid f(P)=0,\text{对于所有}f\in T\}$$

为 n 元多项式 T 的**零点集**。

下面我们介绍射影空间与多项式之间的关系。与仿射空间 $\mathbf{A}^n$ 对应于多项式环 $K[x_1,\cdots,x_n]$ 所不同的是，对于射影空间 $\mathbf{P}^n$，我们需要如下定义的齐次多项式。

考虑 $K[x_0,\cdots,x_n]$ 中的单项式

$$f(x_0,\cdots,x_n)=a\prod_{i=0}^{n}x_i^{d_i}=a\,x_0^{d_0}\cdots x_n^{d_n},$$

其中 d_i 是非负整数。如果 $\sum_{i=0}^{n}d_i=d$，我们称 $f(x_0,\cdots,x_n)$ 是 ***d* 次单项式**，称 d 为单项式的**次数**。$K[x_0,\cdots,x_n]$ 中的多项式 $g(x_0,\cdots,x_n)$ 由若干同一次数是 d 单项式构成，我们称为 ***d* 次齐次多项式**，或简称**齐次多项式**。

显然，如果 $K[x_0,\cdots,x_n]$ 中的多项式 $g(x_0,\cdots,x_n)$ 为 d 次齐次多项式，对于任意的 $\lambda\neq 0$，我们有 $g(\lambda x_0,\cdots,\lambda x_n)=\lambda^d g(x_0,\cdots,x_n)$，进而

$$g(x_0,\cdots,x_n)=0 \Leftrightarrow g(\lambda x_0,\cdots,\lambda x_n)=0 \text{。}$$

因此，对于齐次多项式，其变量的取值只与其等价类 $[x_0,\cdots,x_n]$ 有关，而与具体坐标无关。这也就说明了对于射影空间，我们为什么要考虑齐次多项式，而不是一般的多项式。

例 9.1,3　$g(x,\ y)=4x^7+3x^5y^2+xy^6$ 为 7 次齐次多项式。

类似于仿射空间里代数簇的定义，我们有：

定义 9.1.2b　K 为代数闭域，设 $K[x_0,\cdots,x_n]$ 为 K 上的 n 元多项式环，f 是 $K[x_1,\cdots,x_n]$ 中的一个齐次多项式，我们称 $Z(f)=\{P\in \mathbf{P}^n \mid f(P)=0\}$ 为 n 元多项式 f 的**零点集**。

类似地，如果存在 $K[x_0,\cdots,x_n]$ 的由齐次多项式构成的子集 T，我们称 $Z(T)=\{P\in \mathbf{P}^n \mid f(P)=0$ 对于所有 $f\in T\}$ 为 n 元多项式 T 的**零点集**。

例 9.1.4 我们考虑复数域 $\mathbf{C}$ 上的二元多项式环 $\mathbf{C}[x,y]$，设中 $\mathbf{C}[x,y]$ 一个多项式

$$f(x,y)=(x^2+1)(y^2+1)$$

根据定义有，

$$f(x,y)=(x^2+1)(y^2+1)=0$$

当且仅当 $x^2+1=0$ 或者 $y^2+1=0$，进而有 $Z(f)=\{(\pm i,a),(b,\pm i)\mid a,b\in \mathbf{C}\}$。

若考虑 $\mathbf{C}[x\ y$ 的子集 $T=\{(x^2+1)+(y^2+1),\ (x^2+1)-(y^2+1)\}$，则 $(x^2+1)+(y^2+1)=x^2(+\ 1)y^2(+$ 当且仅当 $x^2+1=y^2+1=0$，进而 $Z(\ \mp)\ \{i\ (-i,\ i)\ ,i$。

定理 9.1.1a　（1）设 $T=\{f_1,\cdots,f_r\}$ 是 $K[x_1,\cdots,x_n]$ 的子集，则 $Z(T)=\bigcap_{i=1}^{r} Z(f_i)$；

（2）设 $f=f_1\cdots f_r$ 是 $K[x_1,\cdots,x_n]$ 中的一个多项式，则 $Z(f)=\bigcup_{i=1}^{r} Z(f_i)$。

证明：留作习题。

定理 9.1.1b （1）设 $T=\{f_1,\cdots,f_r\}$ 是 $K[x_1,\cdots,x_n]$ 的齐次多项式子集，则 $Z(T)=\bigcap_{i=1}^{r}Z(f_i)$；

（2）设 $f=f_1\cdots f_r$ 是 $K[x_1,\cdots,x_n]$ 中的一个多项式，其中 f，$f_1,\cdots,f_r$ 是齐次多项式，则 $Z(f)=\bigcup_{i=1}^{r}Z(f_i)$。

证明：留作习题。

定义 9.1.3a 设 Y 是 n 维仿射空间 $\mathbf{A}^n$ 的子集，如果存在 $K[x_1,\cdots,x_n]$ 的子集 T，使得

$$Y=Z(T),$$

我们则称 Y 是**代数集**。

定义 9.1.3b 设 Y 是 n 维射影空间 $\mathbf{P}^n$ 的子集，如果存在 $K[x_0,\cdots,x_n]$ 的由齐次多项式构成的子集 T，使得 $Y=Z(T)$，我们则称 Y 是**代数集**。

例 9.1.5 我们考虑 $\mathbf{C}$ 上仿射平面的子集

$$Y=\{(1+i,1-i),(1-i.1+i)\}$$

显然，若定义 $\mathbf{C}[x,y]$ 的子集

$$T=\{x+y-2,xy-2\}$$

根据上述定义有 $Y=Z(T)$，即 Y 是代数集。

定理 9.1.2a 两个代数集的并，任意多个代数集的交，以及空集 ϕ 和整个空间 $\mathbf{A}^n$ 都是代数集。

证明：若 $Y_1=Z(T_1)$，$Y_2=Z(T_2)$，则 $Y_1\cup Y_2=Z(T_1T_2)$，其中 T_1T_2 为 T_1 中元素与 T_2 中元素乘积所构成的集合。具体地，若 $P\in Y_1\cup Y_2$，不妨设 $P\in Y_1$，则一定是 T_1T_2 中每个多项式的零点集；反之，若 $P\in Z(T_1T_2)$ 但 $P\notin Y_1$，则存在 $f\in T_1$ 使得 $f(P)\neq 0$，进而对于每个 $g\in T_2$，由 $fg(P)=0$ 可得 $g(P)=0$，故 $P\in Y_2$。

若 $Y_\alpha=Z(T_\alpha)$ 是一族代数集，则

$$\bigcap_\alpha Y_\alpha=Z(\bigcup_\alpha T_\alpha)$$

即 $\bigcap_\alpha Y_\alpha$ 是代数集。

考虑 $K[x_1,\cdots,x_n]$ 中任意非零常数 $c\in K^*$ 以及零多项式 0，我们有 $\phi=Z(c)$，$\mathbf{A}^n=Z(0)$。

定理 9.1.2b 两个代数集的并，任意多个代数集的交，以及空集 ϕ 和整个空间 $\mathbf{P}^n$ 都是代数集。

最后，我们介绍一下仿射空间 $\mathbf{A}^n$ 与射影空间 $\mathbf{P}^n$ 之间的映射关系。

一，首先，对于 $K[x_1,\cdots,x_n]$ 中的任意一个多项式 $f(x_1,\cdots,x_n)$，设其单项式最高次数为 m，我们可以通过变换：

$$\Phi_i: f(x_0,\cdots,x_{i-1},x_{i+1},\cdots,x_n)\mapsto x_i^m f(\frac{x_1}{x_i},\cdots,\frac{x_n}{x_i}),$$

将其变换为 m 次齐次多项式。具体地。对于给定的 i，其中先将变量 $x_1,\cdots,x_n$ 记为 $x_0,\cdots,x_{i-1},x_{i+1},\cdots,x_n$，然后作用上述 Φ_i，进而得到 $K[x_0,\cdots,x_n]$ 中的一个齐次多项式。

例 9.1.6　试将欧氏平面上

(1)直线方程：$ax+by+c=0$

(2)椭圆方程：$\dfrac{x^2}{a^2}+\dfrac{y^2}{b^2}=1$

化成实数域上的射影平面上的齐次坐标方程为。

解：　(1)我们将 $x=X/Z,\ y=Y/Z$ 代入 $ax+by+c=0$ 得

直线的齐次坐标方程为：$aX+bY+cZ=0$.

(2)同样地，代入 $\dfrac{x^2}{a^2}+\dfrac{y^2}{b^2}=1$ 有：

椭圆方程的齐次坐标方程为：$\dfrac{X^2}{a^2}+\dfrac{Y^2}{b^2}=Z^2$.

二，对于两类空间，我们也有相应的变换。若定义射影空间 $\mathbf{P}^n$ 的子集：

$$H_i=\{[a_0,\cdots,a_n]\,|\,[a_0,\cdots,a_n]\in \mathrm{P^n},\ a_i=0\}\text{ 以及}$$

$$U_i=\mathbf{P}^n\setminus H_i$$

直观地讲，U_i 是 $\mathbf{P}^n$ 中 i 坐标不为 0 的点构成的子集。

我们有 $\mathbf{P}^n=\bigcup_{i=0}^{n}U_i$，因为 $\mathbf{P}^n$ 中的任意点必有一个坐标不为 0，进而属于某个 U_i。

现在我们可以定义映射 $\varphi_i : U_i \to \mathrm{A}^n$ 如下：

$$\varphi_i[a_0,\cdots,a_{i-1},a_i,a_{i+1},\cdots,a_n]=(\frac{a_0}{a_i},\cdots,\frac{a_{i-1}}{a_i},\frac{a_{i+1}}{a_i},\ldots,\frac{a_n}{a_i})\ 。$$

可以注意到，$\frac{a_j}{a_i}$ 的值只由其所在的等价类唯一确定，而 $[a_0,\cdots,a_{i-1},a_i,a_{i+1},\cdots,a_n]$ 中齐次坐标的选取无关。

例 9.1.7 求欧氏平面上的点(1, 2)在定义在实数域 $\mathbf{R}$ 上的射影平面上的齐次坐标.

解 点(1, 2)为仿射坐标, $Z\neq 0$, $x = X/Z = 1$, $y = Y/Z = 2$.

所以，有 $X = Z$, $Y = 2Z$ 齐次坐标为[Z, $2Z$, Z]，$Z\neq 0$. 即形如[Z, $2Z$, Z]，$Z\neq 0$ 的齐次坐标，例如［1, 2, 1］，［2, 4, 2］，［1.2, 2.4, 1.2］等都是欧氏平面上的点(1, 2)的在射影平面上的齐次坐标.

进一步地，仿照例 9.1.1，我们有 $\varphi_i : U_i \to \mathrm{A}^n$ 是一一映射，其逆映射 $\psi_i : \mathrm{A}^n \to U_i$ 定义为：

$$\psi_i(a_0,\cdots,a_{i-1},a_{i+1},\cdots,a_n)=[a_0,\cdots,a_{i-1},1,a_{i+1},\cdots,a_n]$$

则有 $\varphi_i \circ \psi_i = \mathrm{id}_{U_i}$ ， $\psi_i \circ \varphi_i = \mathrm{id}_{\mathrm{A}^n}$ 。

此外，若对任意 $[a_0,\cdots,a_{i-1},0,a_{i+1},\cdots,a_n]\in H_i$ ，规定：

$$\varphi_i[a_0,\cdots,a_{i-1},0,a_{i+1},\cdots,a_n]=(\frac{a_0}{0},\cdots,\frac{a_{i-1}}{0},\frac{a_{i+1}}{0},\ldots,\frac{a_n}{0})=\infty\ ,$$

则可将上述 $\varphi_i : U_i \to \mathrm{A}^n$，扩展到射影空间 $\mathbf{P}^n$ 中，得到映射 $\varphi_i : \mathbf{P}^n \to \mathbf{A}^n \bigcup \{\infty\}$，且 φ_i 在 U_i 上仍是一一映射。

一般的，对于 $K[x_1,\cdots,x_n]$ 中的任意一个多项式 $f(x_1,\cdots,x_n)$，我们可以按照上述方法将其变换为 $K[x_1,\cdots,x_n]$ 中的一个齐次多项式 $f_{\mathrm{P}}(x_0,x_1,\cdots,x_n)$ 。根据上面的结论，我们可以得到：

定理 9.1.3 ψ_i , Φ_i 定义如上，设 $(a_0,\cdots,a_{i-1},a_{i+1},\cdots,a_n)$ 是 $K[x_1,\cdots,x_n]$ 中的多项式 $f(x_1,\cdots,x_n)$ 的任意零点，即：

$$(a_0,\cdots,a_{i-1},a_{i+1},\cdots,a_n)\in Z(f)=\{P\in \mathrm{A}^n \mid f(P)=0\}\ ,$$

则 $\psi_i(a_0,\cdots,a_{i-1},a_{i+1},\cdots,a_n)$ 是 $K[x_0,\cdots,x_n]$ 中的齐次多项式 $\Phi_i(f)$ 的零点，即：

$$\psi_i(a_0,\cdots,a_{i-1},a_{i+1},\cdots,a_n)\in Z(\Phi_i(f))=\{P\in\mathbf{P}^n\mid\Phi_i(f)(P)=0\}。$$

证明：留作习题，略。

这个定理指出了如何由仿射空间中的零点，构造对应的射影空间的零点。一个自然的问题随之而来，上述方法能否构造出射影空间中对应的所有零点？一般而言，射影空间中对应的零点会更多一些，我们可以通过一个例子说明这一点。

例 9.1.7 考虑欧氏平面上的双曲线方程：

$$x^2-y^2=1 \qquad (1)$$

若将 $x = X/Z,\ y = Y/Z$ 代入，我们有：$X^2-Y^2=Z^2$。 (2)

根据上述 $\psi_i:\mathbf{A}^n\to U_i$，构造 $\psi_2:\mathbf{A}^2\to U_2$，对于（1）（2）的零点集，我们可建立对应关系：$(x,y)\mapsto[x,y,1]$。

也就是说，任给 $\mathbf{A}^2$ 中满足（1）的点 (x,y)，我们可以构造 $\mathbf{P}^2$ 中满足（2）的点 $[x,y,1]$。

但值得注意的是，$[1,1,0]$ 满足（2），但却不存在 $\mathbf{A}^2$ 中满足（1）的点在上述 $\psi_2:\mathbf{A}^2\to U_2$ 下与之对应。因此，我们把 $[1,1,0]$ 也看作（1）中的点，即无穷远点。

实际上，若设 $\frac{1}{0}=\infty$，我们也可以认为 $\psi_2(\infty,\infty)=[\infty,\infty,1]=[1,1,0]$。此外，若将点 (∞,∞) 带入（1）的变形：

$$x^2=y^2+1 \qquad (1')$$

则有 $\infty^2=\infty^2+1$，即 $\infty=\infty+1$，是合理的。（这里认为 $\mathbf{R}\cup\{\infty\}$ 是半群）

因此，对于给定的 i 以及 $\psi_i:\mathbf{A}^n\to U_i$，对于定理 9.1.3，我们将 $\mathbf{P}^n$ 中不能由 $\mathbf{A}^n$ 中相应零点经 ψ_i 生成的零点构成的集合，即 $Z(\Phi_i(f))\setminus\psi_i(Z(f))$，称为多项式 f 的**无穷远点**。至此，可知射影空间的零点集会比仿射空间多出若干无穷远点。在 9.3 节我们将发现，恰恰是射影空间中这些无穷远点使得零点集具有一定的代数结构，从而更加便于进一步分析零点集的结构与性质。实际上，也因为此，在代数几何学中通常考虑射影空间。

习题 9.1

A 组

1. 证明定理 9.1.1a。
2. 证明定理 9.1.2b。
3. 求下列多项式或其次多项式集合的零点集（复数域）。

(1)$\{x^4-1, x-1\}$；(2)$\{x^2-3y^2-13, 2x^2-7y^2-22, xy+10\}$.

(3)$\{x^2-y^2-1,\ x^2+y^2-3\}$;(4)$\{X^2-Y^2-Z^2, X^2+Y^2-3Z^2\}$

4. 将下列多项式化为其次多项式：

(1) $4x^2+27y^3$ ； (2) $y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6$。

5. 证明：$\varphi_i: U_i \to \mathbf{A}^n$ 是一一映射，且 $\varphi_i \circ \psi_i = \mathrm{id}_{U_i}$， $\psi_i \circ \varphi_i = \mathrm{id}_{\mathbf{A}^n}$。

B 组

6. 指出例 9.1.7 在 φ_0, φ_1 下的无穷远点。

7. 证明定理 9.1.3.

9.2* 代数曲线

这一节我们主要介绍代数簇和代数曲线的概念，首先引入仿射空间上的一类拓扑——Zariski 拓扑。这部分内容用*号进行了标注，读者可根据情况宣读。

定义 9.2.1 设我们定义代数集的补集为 $\mathbf{A}^n$ 中的开集，根据上述结论，我们可得两个开集的交是开集，任意多个开集的并是开集，空集 ϕ 和整个空间 $\mathbf{A}^n$ 都是开集。进而 $\mathbf{A}^n$ 中的此类开集定义构成拓扑，我们称之为 **Zariski 拓扑**。

定义 9.2.2 拓扑空间 X 的非空子集 Y，若果 Y 不能表示为两个 Y 真闭子集的并，即 Y 不能表示为 $Y=Y_1 \bigcup Y_2$，其中为两个 Y 真闭子集 Y_1， Y_2，则称 Y 是**不可约的**。对于 $\mathbf{A}^n$ 上 Zariski 拓扑，我们称 $\mathbf{A}^n$ 中的不可约闭集为**仿射代数簇**，或**仿射簇**。仿射簇的开子集称为**拟仿射簇**。

定义 9.2.3 对于 $\mathbf{A}^n$ 的任意子集 Y，我们定义 Y **在** $\mathbf{A}^n$ **中的理想**为

$$I(Y)=\{f \in K[x_1,\cdots,x_n] \mid f(P)=0, \text{对于所有} P \in Y\}。$$

我们容易验证， $I(Y)$ 是 $K[x_1,\cdots,x_n]$ 的理想。

定理 9.2.1 （1）若 $T_1 \subseteq T_2$ 是 $K[x_1,\cdots,x_n]$ 的两个子集，则 $Z(T_1) \supseteq Z(T_2)$；

（2）若 $Y_1 \subseteq Y_2$ 是 $\mathbf{A}^n$ 的两个子集，则 $I(Y_1) \supseteq I(Y_2)$；

（3）若 Y_1，Y_2 是 $\mathbf{A}^n$ 的任意两个子集，则 $I(Y_1 \cup Y_2) \supseteq I(Y_1) \cap I(Y_2)$。

（4）若 Y 是 $\mathbf{A}^n$ 的任意子集，则 $Z(I(Y)) = \overline{Y}$。

证明：（1）（2）（3）的证明比较直接，留作习题。下面我们证明（4）。

显然，$Y \subseteq Z(I(Y))$，而右边是闭集，故 $\overline{Y} \subseteq Z(I(Y))$。另一方面，设 W 是任一包含 Y 的闭集，则有 $W = Z(A)$，A 为 $K[x_1, \cdots, x_n]$ 的某一理想。于是 $Z(A) \supseteq Y$，由（2）有，$I(Z(A)) \subseteq I(Y)$, 但显然 $A \subseteq I(Z(A))$。由（1）可知 $W = Z(A) \supseteq Z(I(Y))$，因此 $Z(I(Y)) = \overline{Y}$。

例 9.2.1 根据定义 $\mathbf{A}^n$ 不可约的，因为其对应 $K[x_1, \cdots, x_n]$ 的零理想，而零理想是素理想。$\mathbf{A}^n$ 的子集 $\{(1, a_2, \cdots, a_n) \mid a_i \in K, 2 \le i \le n\}$ 也是不可约的，因为其对应的多项式 $f(x_1, \cdots, x_n) = x_1 - 1$ 是不可约的，进而 f 生成素理想。

下面我们介绍射影空间中代数簇等概念。

定义 9.2.4　设我们定义代数集的补集为 $\mathbf{P}^n$ 中的开集，根据上述结论，我们可得两个开集的交是开集，任意多个开集的并是开集，空集 ϕ 和整个空间 $\mathbf{P}^n$ 都是开集。进而 $\mathbf{P}^n$ 中的此类开集定义构成拓扑，我们称之为 **Zariski 拓扑**。

定义 9.2.5　拓扑空间 X 的非空子集 Y，若果 Y 不能表示为两个 Y 真闭子集的并，即 Y 不能表示为 $Y = Y_1 \cup Y_2$，其中为两个 Y 真闭子集 Y_1，Y_2，则称 Y 是**不可约的**。对于 P^n 上 Zariski 拓扑，我们称 A^n 中的不可约闭集为**射影代数簇**，或**射影簇**。仿射簇的开子集称为**拟射影簇**。

同样地，对于 P^n 的任意子集 Y，我们定义 ***Y* 在 $\mathbf{P}^n$ 中的理想**为

$$I(Y) = \{ f \in K[x_0, \cdots, x_n] \mid f \text{是齐次多项式，且对于所有} P \in Y \text{有} f(P) = 0 \}。$$

我们同样容易验证，$I(Y)$ 是 $K[x_0, \cdots, x_n]$ 的理想。值得注意的是，与仿射空间中的定义有所不同，这里理想的定义为齐次多项式。

定义 9.2.6 对于仿射（射影）代数集 Y，我们称商环 $K[x_1, \cdots, x_n] / I(Y)$（$K[x_0, \cdots, x_n] / I(Y)$）为 Y 的**仿射（射影）坐标环**，记为 $A(Y)$。

定理 9.2.2　代数集是不可约的，当且仅当它的理想是素理想。

证明：必要性。若 Y 不可约，考虑多项式环 $K[x_1,\cdots,x_n]$ 中的多项式 f，g 满足 $fg \in I(Y)$，则 $Y \subseteq Z(fg) = Z(f) \cup Z(g)$，于是 $Y = (Y \cap Z(f)) \cup (Y \cap Z(g))$，右端均为 Y 的闭子集。因为 Y 不可约，则 $Y = Y \cap Z(f)$ 或 $Y = Y \cap Z(g)$，进而 f 或 $g \in I(Y)$，$I(Y)$ 是素理想。

充分性。若 T 是素理想，且 $Z(T) = Y_1 \cup Y_2$，则 $T = I(Y_1) \cap I(Y_2)$，进而 $T = I(Y_1)$ 或者 $T = I(Y_2)$，因此 $Z(T) = Y_1$ 或者 $Z(T) = Y_2$，故 $Z(T)$ 不可约。

实际上，回顾关于仿射空间 A^n 的定理 9.2.1 和 9.2.2，类似的结论对于射影空间的情形依然成立。我们在此就不赘述，有兴趣的读者可以尝试叙述并证明。此外，回顾 9.1 节给出的映射 φ_i，我们有如下的结论。

定理 9.2.3 映射 φ_i 是 U_i 到 $\mathbf{A}^n$ 的同胚映射。

证明：留作习题。

下面我们介绍代数曲线，代数曲线是一类重要的代数簇，我们主要介绍代数曲线的相关性质。

首先我们回顾第一章中，拓扑空间维数的定义。对于代数簇，我们给出一般的代数曲线定义：

定义 9.2.7 设 V 是仿射（射影）代数簇，**V 的维数**定义为 V 在其仿射（射影）空间的 Zariski 拓扑中的维数，记作 $\dim(V)$。我们称 1 维的仿射（射影）代数簇为**代数曲线**。

值得指出的是，$\dim(V)$ 作为拓扑空间的维数，恰恰是 V 的仿射（射影）坐标环 $A(V)$ 中不可约素理想升链的最大长度，也称为 **Krull 维数**，即满足：

$$p_0 \subseteq p_1 \subseteq \cdots \subseteq p_{n-1} \subseteq p_n，\text{其中} \{p_i\}_{0\le i\le n} \text{为 } I \text{ 中互不相同的素理想}$$

的最大非负整数 n，记为 $\dim(I)$。有兴趣的读者可以参照定理 9.2.1 和 9.2.2 以及一些初等交换代数的知识给出证明。

此外，倘若限定代数曲线 V 在二维仿射空间 A^2 或二维射影空间 P^2 中，我们称之为**平面代数曲线**。

根据拓扑空间维数，以及代数簇对应中多项式环中的素理想，我们可以得到以下结论。关于推导过程，有兴趣的读者可以参考[AG, GTM 52]。

命题 1：*代数簇 C 是仿射（射影）空间中的代数曲线，当且仅当其理想 $I(C)$ 是一维（Krull 维数）素理想。*

命题 2：*代数簇 C 是二维仿射空间 A^2 或二维射影空间 P^2 中的代数曲线，当且仅当其理想 $I(C)$ 是一维（Krull 维数）素理想。*

也就是说，二维空间中的代数曲线，可以由一个多项式环 $K[x,y]$ 或 $K[X,Y,Z]$ 中的不可约多项式确定。实际上，根据定理 9.1.1，对于可约的多项式 $f = f_1 \cdot \cdots \cdot f_r$，其对应的代数簇为 $Z(f)=\bigcup_{i=1}^{r} Z(f_i)$，可以表示为不可约多项式零点集的并。所以，我们主要讨论对于不可约多项式以及其对应的代数曲线的性质。

此外，对于 K 的子域 F，若代数簇 C 对应的理想 $I(C)$ 是 $F[x_1,\cdots,x_n]$ 中的素理想，我们称 C 为 F **-代数曲线**。

例 9.2.2　考虑有限域 F_4 上二维仿射空间 $\mathbf{A}^2$ 中的代数方程：

$$C:\ y^2+y=x^3$$

易知 C 的理想为 $<x^3-y^2-y>$，而 x^3-y^2-y 为 F_4 代数闭包 $\bigcup_{i=1}^{\infty} F_{2^i}$（参 8.6 节）上的不可约多项式，故而是 $\mathbf{A}^2$ 中的一条代数曲线。

例 9.2.3　考虑我们所熟悉的椭圆方程：

$$x^2+9y^2=1。$$

其对应的理想为：$<x^2+9y^2\text{-}1>$，在实数域内不可分解，进而为实代数曲线。但在特征为 3 的有限域 F_{3^i} 内可分解为 $x^2+9y^2\text{-}1=x^2+6xy+9y^2\text{-}1=(x+3y+1)(x+3y-1)$，根据定理 9.1.1，对应于两条曲线 $x+3y+1$ 与 $x+3y-1$ 的并。

定义 9.2.8　设 C 为仿射空间 $\mathbf{A}^n$ 中代数曲线，$K[x_1,\cdots,x_n]$ 中多项式 $f_1,\cdots,f_m$ 生成其理想 $I(C)$，给定 C 上一点 P，如果雅克比（Jacobian）矩阵

$$\left(\frac{\partial f_j}{\partial x_i}\right)_{1\le j\le m,1\le i\le n}$$

在 P 点的秩为 n-1，我们称 C 在 P 点**非奇异（光滑）**的，否则称之为**奇异**的。若 C 在其上所有点都是非奇异（光滑），我们则称 C 是**非奇异（光滑）**的。

这里我们有一点需要说明。上述雅克比矩阵的偏导数定义为

$$\partial x^n = nx^{n-1}$$

注意，对于特征为素数 p 的域，我们有 $\partial x^p = px^{p-1}=0$。

我们知道，给定 $\mathbf{A}^n$ 中代数曲线 C，由于 $I(C)$ 是素理想，进一步由其 Krull 维数为 1 知 $I(C)$ 为极大理想，从而 C 的仿射（射影）坐标环 $A(C)$（作为对于 $I(C)$ 的商环）是域，根据第八章的知识可知，该扩张是超越扩张，称为 C 的**代数函数域**，记为 $K(C)$。

对于任意上述的扩域 $K(C)$，都有一个极为重要的参数——**亏格**（genus）刻画其性质。关于亏格的介绍，有兴趣的读者可以参考代数函数以及代数几何的书籍[9,11,16]，这里由于篇幅原因就不多叙述了。

最后，我们给出一类极为重要的代数曲线——椭圆曲线的定义。

定义 9.2.9 如果代数曲线 C 的亏格为 1，我们则称 C 为椭圆曲线。

给定任意椭圆曲线 C，我们有一个亏格为 1 的域 $K(C)$，进而可以由 $K(C)$唯一确定如下的 Weierstrass 方程：

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

其中 $a_1, a_2, a_3, a_4, a_6 \in K$ 。该方程称为椭圆曲线 C 的 Weierstrass 方程。进而，我们可以得到：椭圆曲线是由非奇异 Weierstrass 方程确定的一种曲线。

学习椭圆曲线之前我们先简要介绍一下椭圆曲线的历史背景. 首先要明确：椭圆曲线的形状并不是椭圆. 椭圆曲线的研究源于椭圆积分，至于椭圆积分的背景知识和怎样由椭圆积分导出椭圆曲线，本书不作详细介绍，感兴趣的读者可以参考代数几何方面的教材. 从下一节起，我们将从 Weierstrass 方程的角度直接给出椭圆曲线的定义.

习题 9.2

A 组

1. 证明定理 9.2.1(1)(2)(3).

B 组

2*. 对于理想 A，定义 A 的**根**为 $\sqrt{A} = \{ f \in A \mid \exists r \in Z^+ : f^r \in A \}$

试证明：对于 $K[x_1, \cdots, x_n]$ 的任意理想 A， $I(Z(A)) = \sqrt{A}$

3. 定义满足 $I(Z(A)) = \sqrt{A}$ 的理想 A 为**根式理想**，证明： A^n 的代数集与 $K[x_1, \cdots, x_n]$ 的根式理想之间存在一一对应关系：

$$Y \mapsto I(Y), A \mapsto Z(A)$$

4. 证明定理 9.2.3.

9.3 Weierstrass 方程与椭圆曲线

我们在前两节介绍了仿射、射影空间与其中代数簇的相关概念和性质，引出了一类特殊的代数簇——代数曲线，进而有得到了一类特殊的代数曲线——椭圆曲线，即由 Weierstrass 方程所确定的曲线。本节将主要讨论 Weierstrass 方程的有关性质。

定义 9.3.1　设 K 为域，$a_1,a_2,a_3,a_4,a_6 \in K$，形如

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{9.3.1}$$

的方程称为**域 K 上的 Weierstrass 方程**，通常记为 $E(K)$，a_1,a_2,a_3,a_4,a_6 称为 Weierstrass 方程的**系数**. 这里的域 K 可以是任何域，既包括实数域 R、复数域 C、有限域，还可以是本书未涉及的函数域、局部域等。

我们可以这样来记忆 Weierstrass 方程系数的下标，设 x,y,a_1,a_2,a_3,a_4,a_6 的权值如表 9.3.1 所示.

表 9.3.1　Weierstrass 方程系数权值表

x 的权值	2
y 的权值	3
a_i 的权值	i

则 Weierstrass 方程的每一项权值都是 6，这也是为什么没有系数 a_5 的原因.

如果域 K 的特征不为 2，令 $\eta = y + (a_1x + a_3)/2$，消去 y 的二次项，方程(9.3.1)可化为

$$\eta^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}, \tag{9.3.2}$$

其中

$$\begin{cases} b_2 = a_1^2 + 4a_2 \\ b_4 = a_1a_3 + 2a_4 \\ b_6 = a_3^2 + 4a_6 \end{cases} \tag{9.3.3}$$

如果域 K 的特征不为 2、3，令 $\xi = x + b_2/12$，消去 x 的二次项，方程(9.3.2)可化为

$$\eta^2 = \xi^3 - \frac{c_4}{48}\xi - \frac{c_6}{864}, \tag{9.3.4}$$

其中

$$\begin{cases} c_4 = b_2^2 - 24b_4 \\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6 \end{cases} \tag{9.3.5}$$

另定义

$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2, \tag{9.3.6}$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \tag{9.3.7}$$

系数 b 和 c 的下标也可理解成它们的权值. 我们将式(9.3.1), (9.3.2)和(9.3.4)分别称为 Weierstrass 方程的 a 形式、b 形式和 c 形式. 容易验证，系数定义(9.3.3), (9.3.5), (9.3.6)和(9.3.7)式对所有 Weierstrass 方程都成立, 不管域 K 的特征是否为 2 或 3.

可以证明（留作练习）, 当域 K 的特征不为 2 时, Δ 等于 b 形式的 Weierstrass 方程右边多项式的判别式的 16 倍, 即

$$\Delta = 16D\left(x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}\right).$$

所以当域 K 的特征不为 2 时, K 上的 Weierstrass 方程(9.3.1)有重根当且仅当 $\Delta = 0$.

当 $\Delta \neq 0$，我们定义

$$j = c_4^3 / \Delta, \tag{9.3.8}$$

称 j 为 Weierstrass 方程(9.3.1)的 j **不变量**, 可记作 $j(E(k))$.

定义

$$\kappa = 2y + a_1x + a_3, \tag{9.3.9}$$

当域 K 的特征不为 2 时有 $\kappa = 2\eta$ (不恒为零). 当域 K 的特征为 2 时, 我们有

$$\begin{aligned}
\Delta \neq 0 &\Rightarrow b_2^2b_8 + b_6^2 + b_2b_4b_6 \neq 0 \\
&\Rightarrow a_1^4\left(a_1^2a_6 + a_1a_3a_4 + a_2a_3^2 + a_4^2\right) + a_3^4 + a_1^3a_3^3 \neq 0 \\
&\Rightarrow a_1^6a_6 + a_1^5a_3a_4 + a_1^4a_2a_3^2 + a_1^4a_4^2 + a_3^4 + a_1^3a_3^3 \neq 0 \\
&\Rightarrow a_1\text{和}a_3\text{不能同时为}0.
\end{aligned}$$

因此 $\Delta \neq 0$ 时, 对任意域 K 上的 Weierstrass 方程都有 κ 不恒为零, 于是我们有

$$\kappa^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

通常称 c_4, c_6 和 Δ 为 Weierstrass 方程 $E(K)$ 的**三个基本参数**, 它们的权值分别为 4、6 和 12. 例如方程 $y^2 + y = x^3 - x^2$ 的三个基本参数为 16, −152, −11, 即 $c_4 = 16,\ c_6 = -152,\ \Delta = 11$（请读者自己验证）.

另外, 容易验证, 等式

$$4b_8 = b_2b_6 - b_4^2 \tag{9.3.10}$$

$$1728\Delta = c_4^3 - c_6^2 \tag{9.3.11}$$

$$j = \frac{c_4^3}{\Delta} = 1728 + \frac{c_6^2}{\Delta} \tag{9.3.12}$$

成立（留作练习）.

例 9.3.1 当域 K 的特征不为 2 和 3 时, 对 Weierstrass 方程的 c 形式进行变换, 令 $\eta' = 6^3\eta$, $\xi' = 6^2\xi$, 得到

$$(\eta')^2=(\xi')^3-27\bar{c}_4\xi'-54\bar{c}_6 \tag{9.3.13}$$

注意，我们在参数 c_4,c_6 上加了上划线，这是因为，对于式(9.3.13)给出的 Weierstrass 方程，由式(9.3.5)可知

$$c_4=b_2^2-24b_4=0-24(2-27\bar{c}_4)=1296\bar{c}_4,$$

$$c_6=-b_2^3+36b_2b_4-216b_6=0+0-216(4(-54\bar{c}_6))=46656\bar{c}_6,$$

而对于式(9.3.4)给出的Weierstrass方程，可以验证由式(9.3.5)计算得到的参数 c_4,c_6 与式(9.3.4)中原来的参数 c_4,c_6 是一致的.

例 9.3.2　求下列 Weierstrass 方程

(1) $y^2=x^3+px+q$,

(2) $y^2=x^3+q$,

(3) $y^2=x^3+px$

的三个基本参数 c_4,c_6,Δ.

解

(1) 对 $y^2=x^3+px+q$，我们有 $a_1=0,\ a_2=0,\ a_3=0,\ a_4=p,\ a_6=q$，

$$c_4=b_2^2-24b_4=0-24(2(p))=-48p,$$

$$c_6=-b_2^3+36b_2b_4-216b_6=0+0-216(4(q))=-864q,$$

$$\Delta=\frac{c_4^3-c_6^2}{1728}=\frac{(-48p)^3-(-864q)^2}{1728}=-16(4p^3+27q^2).$$

(2) 对 $y^2=x^3+q$，由(1)的结论,

$$c_4=0,\quad c_6=-864q,\quad \Delta=-432q^2\neq 0,$$

当 $\Delta=-432q^2\neq 0$ 时，有 $j=\dfrac{c_4^3}{\Delta}=0$.

(3) 对 $y^2=x^3+px$，由(1)的结论,

$$c_4=-48p,\quad c_6=0,\quad \Delta=-64p^3,$$

当 $\Delta=-64p^3\neq 0$ 时，有 $j=\dfrac{c_4^3}{\Delta}=\dfrac{(-48p)^3}{-64p^3}=1728$.

以上我们用仿射坐标研究了 Weierstrass 方程. 令 $x=\dfrac{X}{Z},y=\dfrac{Y}{Z}$，方程(9.3.1)可以化为

$$Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3, \tag{9.3.14}$$

其中 $a_1,a_2,a_3,a_4,a_6 \in K$，方程(9.3.14)称为 Weierstrass 方程的**齐次坐标形式**. 同样，齐次坐标下的 Weierstrass 方程也有 *a* 形式（即方程(9.3.14)），*b* 形式和 *c* 形式，其 Δ, j 的定义与仿射坐标下的情况一致.

容易验证，凡是满足方程(9.3.1)的平常点(*x*, *y*)，其齐次坐标(*x*, *y*, 1)一定满足方程(9.3.14)，另外齐次坐标为[0, 1, 0]的无穷远点也满足方程(9.3.14)，且在齐次坐标等价意义下(0, 1, 0)是唯一满足方程(9.3.14)的无穷远点，我们将这个无穷远点记为 *O*，即

$$O=[0,\ 1,\ 0],$$

易知**无穷远点 *O* 在与 *y* 轴平行的直线上**. 由此可见，Weierstrass 方程的齐次坐标形式比仿射坐标形式多包含了一个无穷远点 *O*.

定义 9.3.2 设

$$F(X,Y,Z)=Y^2Z+a_1XYZ+a_3YZ^2-X^3-a_2X^2Z-a_4XZ^2-a_6Z^3,$$

如果对任意齐次坐标点(*X*, *Y*, *Z*)，偏导数 $\frac{\partial F}{\partial X},\frac{\partial F}{\partial Y},\frac{\partial F}{\partial Z}$ 不同时为 0，则称 Weierstrass 方程(9.3.14)为**非奇异的**或**光滑的**，否则就称之为**奇异的**.

我们不加证明地给出：

定理 9.3.1 域 K 上的 Weierstrass 方程 $E(K)$ 为非奇异的充要条件是 $\Delta\neq 0$.

例 9.3.3 求证实数域 $\mathbf{R}$ 上的 Weierstrass 方程 $Y^2Z=X^3$ 为奇异的.

证明 设 $F(X,Y,Z)=Y^2Z-X^3$，则有

$$\frac{\partial F}{\partial X}=-3X^2,\quad \frac{\partial F}{\partial Y}=2YZ,\quad \frac{\partial F}{\partial Z}=Y^2$$

在点(0, 0, 1)处 $\frac{\partial F}{\partial X},\frac{\partial F}{\partial Y},\frac{\partial F}{\partial Z}$ 同时为 0，所以域 $\mathbf{R}$ 上的 Weierstrass 方程 $Y^2Z=X^3$ 是奇异的. 也可以用定理 9.2.1 来证明：方程 $Y^2Z=X^3$ 的系数 a_1,a_2,a_3,a_4,a_6 全为 0，所以 $\Delta=0$，因此它是奇异的.

下面我们介绍由 Weierstrass 方程所定义的椭圆曲线。

定义 9.3.3 设 K 为域，0 为 K 的零元，$\bar{K}$ 为 K 的代数闭域，K 上的 Weierstrass 方程

$$Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3$$

为非奇异的（即满足 $\Delta\neq 0$），M 为 $\bar{K}$ 上的射影平面，则 M 上满足方程(9.3.14)的所有点(*X*, *Y*, *Z*)组成的集合称为**域 K 上的椭圆曲线**，记为 $E(\bar{K})$，即

$$M=\{(X,Y,Z)\mid X,Y,Z\in\bar{K}\}\setminus\{0,0,0\},$$

$$E(\bar{K})=\{(X,Y,Z)\in M\mid Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3\}.$$

定义 9.3.3 用 Weierstrass 方程的齐次坐标形式给出了椭圆曲线的定义，根据 9.1 节我们可以知道，Weierstrass 方程的齐次坐标形式只比 Weierstrass 方程的仿射坐标形式多包含一个无穷远点 O，因此我们还可以用 Weierstrass 方程的仿射坐标形式给出椭圆曲线的定义.

定义 9.3.4 设 K 为域，0 为 K 的零元，$\bar{K}$ 为 K 的代数闭域，K 上的 Weierstrass 方程

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$$

为非奇异的（即满足$\Delta\neq 0$），则仿射平面$\bar{K}^2$上满足方程（9.3.14）的所有点(x, y)加上无穷远点$O=[0,1,0]$组成的集合称为**域K上的椭圆曲线**，记为$E(\bar{K})$，即

$$E(\bar{K})=\{(x,y)\in\bar{K}^2 \mid y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6\}\cup\{O\}.$$

9.1 节中已经指出，平常点的仿射坐标(x,y)与齐次坐标(X,Y,Z)（等价齐次坐标看成一个坐标）存在一一对应关系，因此椭圆曲线的两个定义 9.3.3 和 9.3.4 本质上是一致的．为了方便，我们以后讨论椭圆曲线时主要采用定义 9.3.4 的形式.

注意，在上述定义中，$E(\bar{K})$是一系列点的集合，这些点的坐标值在$\bar{K}$内，这就意味着$E(\bar{K})$是相应 Weierstrass 方程在$\bar{K}$（而不是K）内的解集.

定义 9.3.5　设域F是域K的扩域，$E(\bar{K})$是域K上的椭圆曲线，点$P\in E(\bar{K})$，如果P的所有坐标值都在F内或P为无穷点O，则称点P为$E(\bar{K})$上**关于F的有理点**．$E(\bar{K})$上所有关于F的有理点组成的集合记为$E(F)$．以后我们提到“椭圆曲线上的点”都是指椭圆曲线关于某一域的有理点.

注意，$E(\bar{K})$上关于域F的有理点的坐标值不一定是有理数，除非集合F为有理数集.

例 9.3.4　设实数域$\mathbf{R}$上的Weierstrass方程$E(\mathbf{R})$为$Y^2Z=X^3-XZ^2$，求证$E(\mathbf{R})$可以确定一条椭圆曲线，并画出其图像.

解　由$E(\mathbf{R})$的定义可知$a_1=0,\ a_2=0,\ a_3=0,\ a_6=0,\ a_4=-1$，

$$\Delta=-b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6=0-8\big(2(-1)\big)^3-0+0=64>0,$$

所以$E(\mathbf{R})$可以确定一条椭圆曲线．将$E(\mathbf{R})$上所有关于$\mathbf{R}$的有理点画在平面直角坐标系内，我们可得到$E(\mathbf{R})$的图像（注意图像上没有表示出无穷远点），如图 9.2.1 所示.

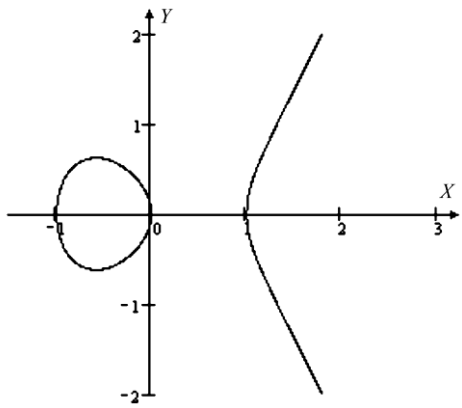

图 9.3.1　$Y^2Z=X^3-XZ^2$ 的图像

同理我们可得到实数域$\mathbf{R}$上的椭圆曲线$Y^2Z=X^3+XZ^2+Z^3$（此椭圆曲线的判别式$\Delta=-b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6=0-8(2(1))^3-27(4)^2+0<0$）的图像，如图 9.4.2 所示.

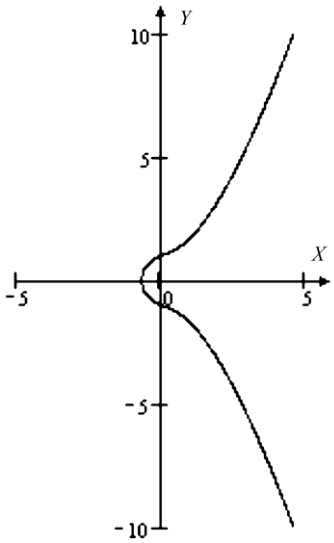

图 9.3.2 $Y^2Z = X^3 + XZ^2 + Z^3$ **的图像**

注意到图 9.4.1 中的椭圆曲线与 X 轴有三个交点，其 $\Delta > 0$，而图 9.4.2 中的椭圆曲线与 X 轴有一个交点，其 $\Delta < 0$．请读者思考：这一结论是否对所有实数域 **R** 上的椭圆曲线都成立？

最后，我们给出实数域 **R** 上几种形如 $y^2 = x^3 + ax + b$ 的椭圆曲线的图像，供读者参考：

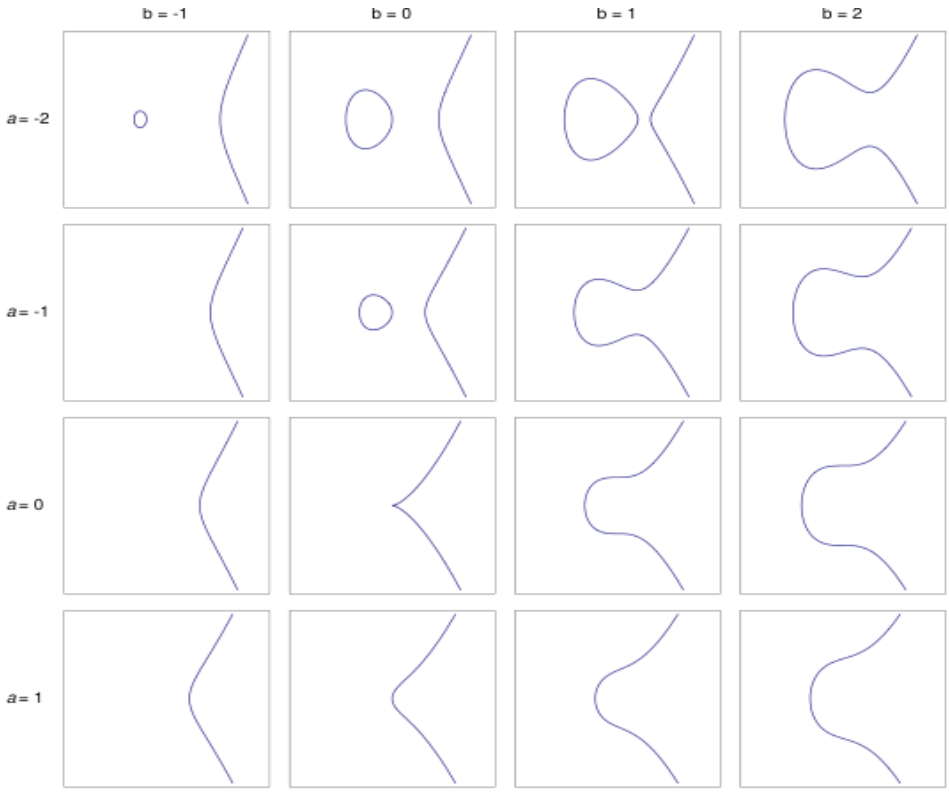

图 9.4.3　实数域上几种形如 $y^2=x^3+ax+b$ 的椭圆曲线的图像（注意：a 和 b 同时为 0 时，方程 $y^2=x^3$ 是奇异的，故不是椭圆曲线）

习题 9.3

A 组

1. 说明 c_4, c_6 和 Δ 的权值分别为 4、6 和 12.

2. 给定域 K 且 $\mathrm{char}K \neq 2,3$，试将 K 上的射影方程：

$$X^3 + Y^3 = cZ^3, c \in K^*$$

表示为仿射平面上的 Weierstrass 方程。

B 组

3. 证明定理 9.3.1.

9.4 椭圆曲线上的群结构

在 9.3 节中我们看到了椭圆曲线的图像，这种图像上点与点之间究竟有什么联系呢？事实上，通过巧妙的定义，椭圆曲线上的点对特定的运算——我们称之为“加法”，可以构成 Abel 群．这就告诉我们，椭圆曲线上点与点之间有着非常深刻的内在联系．正是因为椭圆曲线具有这一优良特性，才使它在数论中有广泛的应用．下面我们给出椭圆曲线上点的加法定义.

Bezout 曾经证明，设 E 是域 K 上的 Weierstrass 方程，点 P 和 Q 是 E 上的点，P 和 Q 的坐标值都在域 K 内，则过点 P 和 Q 的直线与 E 一定交于一点 R，R 的坐标值也在域 K 内，记为 $R = PQ$．如图 9.4.1 所示，如果 $P = Q$，则 R 为 E 在 P 点的切线与 E 的另一个交点，如果过 P 和 Q 的直线在 Q 点与 E 相切，则 $R = PQ = Q$．这就是代数几何里著名的 Bezout 定理.

定义 9.4.1 设 P，Q 是椭圆曲线 E 上的两点，$R = PQ$，O 为无穷远点．如图 9.4.1 所示，点 P 与 Q 的加法定义为

$$P + Q = O(PQ) = OR, \tag{9.4.1}$$

即 R 是过 P 和 Q 的直线与 E 的第三个交点，$P+Q$ 是过 O 与 R 的直线与 E 的第三个交点，图 9.4.1 描述了这种加法的几何意义，图 9.4.1(a)是 $P \neq Q$ 的情况，图 9.4.1(b)是 $P = Q$ 的情况．容易验证，过点 O 和 R 的直线与 Y 轴平行.

注意：椭圆曲线上点 P 与 Q 的“加法”不是 P 与 Q 的相应坐标值之间的加法，要将椭圆曲线上点的加法与解析几何里的向量加法严格区分开来.

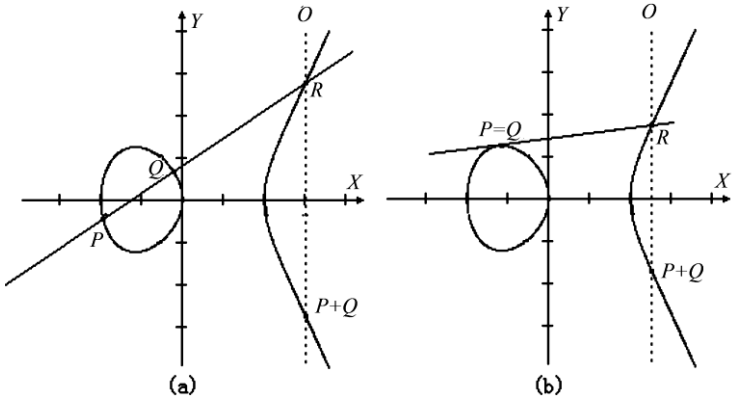

图 9.4.1　椭圆曲线上点的加法

由于在平面解析几何的范围内考虑椭圆曲线问题，因此无穷远点在上面的图中表示不出来，便理解椭圆曲线上的加法定义时要默认它们存在．比如定义中平行于 Y 轴的直线 OR 和椭圆曲线的交点应该有三个，第三个点就在无穷远点．这从另外一个方面说明，在定义椭圆曲线时“人为”引入的那个无穷远点是实际存在的，在引入齐次坐标和射影平面后，这个无穷远点就自然出现了．

还有一点需要注意的是，如果 $E(\bar{K})$ 是定义在域 K 上的椭圆曲线，F 是 K 的扩域，P、Q 是 $E(\bar{K})$ 上的关于 F 的有理点，则过 P、Q 的直线与 $E(\bar{K})$ 的第三个交点一定是 $E(\bar{K})$ 上的关于 F 的有理点．这是因为直线和曲线的联立方程的系数都取自域 F，而方程组有 3 个解，其中两个解就是 P 和 Q，第三个解必为关于 F 的有理点．

需要特别指出的是，点 $P+Q$ 与点 R 不一定关于 X 轴对称，原因是椭圆曲线的图像不一定关于 X 轴对称．例如 $\mathbf{R}$ 上椭圆曲线 $y^2 - xy = x^3 + 1$（如图 9.4.2 所示）．

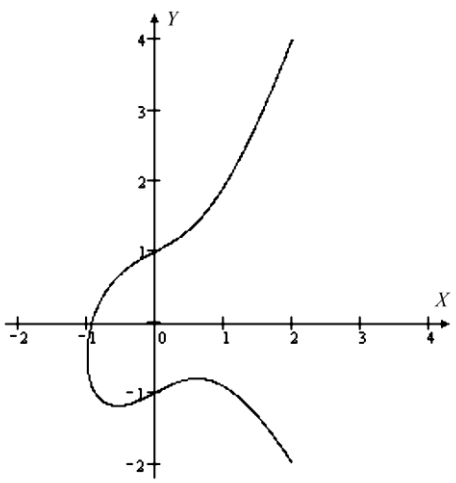

图 9.4.2　椭圆曲线 $y^2 - xy = x^3 + 1$ 的图像

定理 9.4.1　椭圆曲线 E 上点的加法具有如下性质：

(a) 若 P 和 Q 是 E 上任意两点，P 与 Q 的连线 L 交 E 于另一点 R，则；

(b) 对任意 $P\in E$ 有 $P+O=P$；

(c) 对任意 P，$Q\in E$ 有 $P+Q=Q+P$；

(d) 对任意 $P\in E$，E 上存在一点 $-P$，使得 $P+(-P)=O$；

(e) 对于 P 上的任意点 P，Q，R 有 $(P+Q)+R=P+(Q+R)$.

证明

(a) 因为椭圆曲线与无穷远线只有一个交点 O，所以在椭圆曲线上有 $OO=O$ 成立，又由条件知 $R=PQ$，于是 $(P+Q)+R=OR+R=O((OR)R)=OO=O$. 图 9.4.3 给出的 $P+Q+R=O$ 的几种不同情况.

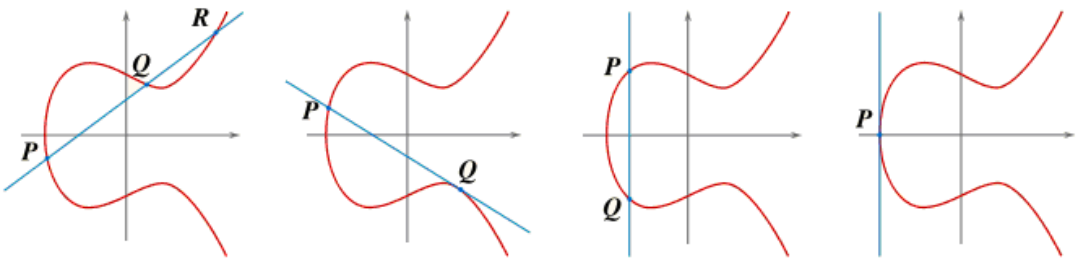

图 9.4.3　椭圆曲线上 $P+Q+R=O$ 的几种不同情况

(b) $P+O=O(PO)=P$.

(c) $P+Q=O(PQ)=O(QP)=Q+P$.

(d) 设 $P'=PO$，则 $PP'=P(PO)=O$，$O(PP')=OO=O$，由式(9.2.15)知 $P+P'=O$，于是 $-P=P'=PO$.

(e) 可通过各种情况进行验证，过程比较繁琐，略去. 感兴趣的读者请参阅文献[10,11].

从定理 9.4.1 可知，椭圆曲线 E 上的点对式(9.4.1)定义的加法满足结合律和交换律，任意点 $P\in E$ 都有负元 $-P$ 存在，且可以将 O 点看作零元，于是椭圆曲线上的点对式(9.4.1)定义的加法构成 Abel 群. 为了简化起见，我们可将 $P+P$ 记为 $2P$，依此类推，

$$mP=P+P+\cdots+P\ (\text{共 } m \text{ 个 } P),$$

称为椭圆曲线上点 P 的 m **倍加**. 与此对应，当 $P\neq Q$ 时，$P+Q$ 称为椭圆曲线上点的**普加**或**点加**.

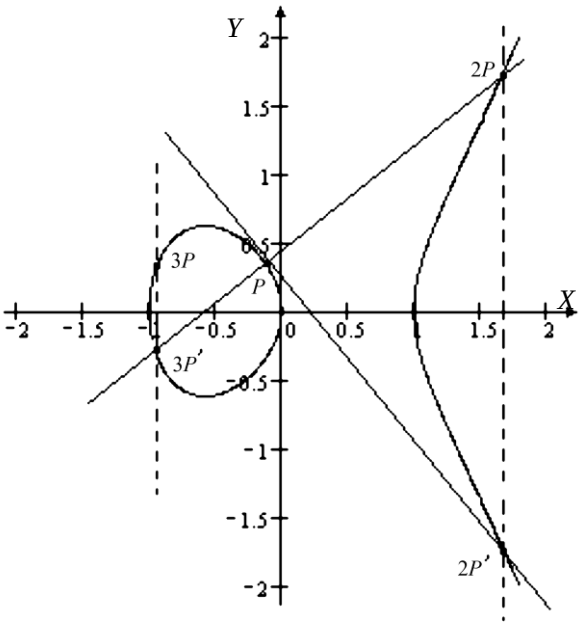

图 9.4.4　椭圆曲线上点 *P* 的倍加

例如，图 9.4.4 给出了椭圆曲线 $y^2 = x^3 - x$ 上一点 P 的 3 倍加的几何意义.

下面我们给出椭圆曲线上点加运算的代数描述.

定理 9.4.2　设椭圆曲线 E 的一般 Weierstrass 方程为

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (\Delta \neq 0).$$

定义 E 为

$$E = \{(x,y) \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\} \tag{9.4.2}$$

设 $P_1 = (x_1, y_1)$，$P_2 = (x_2, y_2)$ 是 E 上的异于无穷远点 O 的两个点，则有

$$-P_1 = (x_1, -y_1 - a_1x_1 - a_3) \quad ,$$

(9.4.3)

如果 $P_2 = -P_1$，则 $P_1 + P_2 = O$；如果 $P_2 \neq -P_1$，设 $P_3 = (x_3, y_3) = P_1 + P_2$，则 x_3, y_3 可由下式给出

$$\begin{cases} x_3 = k^2 + a_1k - a_2 - x_1 - x_2 \\ y_3 = k(x_1 - x_3) - a_1x_3 - y_1 - a_3 \end{cases} \tag{9.4.4}$$

其中参数 k 定义为

$$k = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{如果} x_1 \neq x_2 \text{(对应于点加)} \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & \text{如果} x_1 = x_2 \text{(对应于倍加)} \end{cases} \tag{9.4.5}$$

证明

(1) 设 $P_1=(x_1,y_1)\neq O$，则其负元 $-P_1=(x_1^{'},y_1^{'})$ 为过 P_1 和 O 直线与 E 的第三个交点，显然 $x_1^{'}=x_1$，过 P_1 和 O 直线方程为

$$x=x_1.$$

代入方程(9.4.2)得

$$y^2+(a_1x_1+a_3)y-(x_1^3+a_2x_1^2+a_4x_1+a_6)=0.$$

由 Vieta 定理知

$$y_1+y_1^{'}=-(a_1x_1+a_3),$$

$$y_1^{'}=-y_1-a_1x_1-a_3.$$

于是证明了式(9.4.3)

$$-P_1=(x_1,\ -y_1-a_1x_1-a_3).$$

(2) 如果 $P_2=-P_1$，则 $P_1+P_2=O$．如果 $P_2\neq -P_1$，我们来求 $P_3=(x_3,y_3)=P_1+P_2$，设 $P_3^{'}=(x_3^{'},y_3^{'})=P_1P_2$，即 $P_3^{'}$ 是过 P_1 和 P_2 的直线与 E 的第三个交点，显然 $x_3=x_3^{'}$，考虑过 P_1 和 P_2 的直线

$$L:\ y=kx+t,$$

当 $x_1\neq x_2$ 时，则直线 L 的斜率 k 为

$$k=\frac{y_2-y_1}{x_2-x_1},$$

当 $x_1=x_2$ 时，则直线 L 的斜率 k 为(可以用偏导数来计算，具体过程从略)

$$k=\frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3},$$

将 $y=kx+t$ 代入方程(9.4.2)得

$$x^3-(k^2+a_1k-a_2)x^2+(a_4-2kt-a_1t-a_3k)x+a_6-t^2-a_3t=0.$$

由 Vieta 定理知

$$x_1+x_2+x_3=k^2+a_1k-a_2,$$

即

$$x_3=k^2+a_1k-a_2-x_1-x_2,$$

代入方程 $y=kx+t$ 得

$$y_3' = -(kx_3+t) - a_1x_3 - a_3 .$$

根据式(9.4.3)

$$\begin{aligned} y_3 &= -y_3' - a_1x_3 - a_3 \\ &= -(kx_3+t) - a_1x_3 - a_3 \\ &= -(kx_3 + y_1 - kx_1) - a_1x_3 - a_3 \\ &= k(x_1 - x_3) - a_1x_3 - y_1 - a_3 , \end{aligned}$$

于是证明了式(9.2.18)

$$\begin{cases} x_3 = k^2 + a_1k - a_2 - x_1 - x_2 \\ y_3 = k(x_1 - x_3) - a_1x_3 - y_1 - a_3 \end{cases} .$$

例 9.4.1 椭圆曲线 E: $y^2+xy=x^3+a_2x^2+a_6$ ($\Delta\neq 0$，$a_2, a_6 \in K$, K 的特征为 2)上点的加法. 设 $P_1=(x_1, y_1)$，$P_2=(x_2, y_2)$ 是 E 上的异于无穷远点 O 的两个点，则有

$$-P_1 = (x_1, y_1+x_1) ,$$

如果 $P_2=-P_1$，则 $P_1+P_2=O$；如果 $P_2\neq -P_1$，设 $P_3=(x_3, y_3)=P_1+P_2$，则当 $x_1\neq x_2$ 时，x_3, y_3 可由下式给出

$$\begin{cases} x_3 = \left(\dfrac{y_2+y_1}{x_2+x_1}\right)^2 + \dfrac{y_2+y_1}{x_2+x_1} + a_2 + x_1 + x_2 \\ y_3 = \dfrac{(y_2+y_1)(x_1+x_3)}{x_2+x_1} + x_3 + y_1 \end{cases} ,$$

当 $x_1=x_2$ 时，x_3, y_3 可由下式给出

$$\begin{cases} x_3 = x_1^2 + \dfrac{a_6}{x_1^2} \\ y_3 = x_1^2 + (x_1 + \dfrac{y_1}{x_1})x_3 + x_3 \end{cases}$$

需要指出的是，本节定义的域 K 上椭圆曲线 E 上点的加法群称为 **Mordell-Weil 群**，记为 $E(K)$。

其实发现这个群结构的时间比 Mordell 和 Weil 要早，可以追溯到 Poincare 甚至 Abel. 这个群之所以被称为 Mordel-Weil 群，是因为 Mordell 最早给出了有理域上椭圆曲线 Mordell-Weil 群上有限生成定理，而 Weil 推广了他的结果. 我们这里有必要指出椭圆曲线乃至算术几何中极为著名的 Mordell-Weil 定理：

设 K 为代数数域，E 为 K 上的椭圆曲线，则 $E(K)$ 是有限生成的交换群。

该定理表明，存在 E 上的有限多 r 的点 $P_1,\cdots,P_r$ 使得

$$E(K)\cong E(K)_{\text{tors}}\times \mathbf{Z}P_1\times\cdots\times\mathbf{Z}P_r\cong E(K)_{\text{tors}}\times\mathbf{Z}^r$$

其中 $E(K)_{\text{tors}}$ 是 $E(K)$ 的扭子群（参 6.2 节习题 6）并且是有限群。

而对于有限域 K 上的椭圆曲线 E，由于 $E(K)\subset K\times K$，进而 $E(K)$ 是有限的。

在数论有关的实际计算以及编码、密码学中，我们常用到有限域（在某些情况下也会涉及到一些 p-adic 域和复数域）．有限域上的椭圆曲线和 p-进域上的椭圆曲线没有直观的图形表示，复数域上的椭圆曲线的图形是个三维空间中的环面．在这些情况下思考问题会缺乏直观性，此时最好借用实数域上椭圆曲线的图形来支持我们的直觉.

习题 9.4

A 组

1．给定有理数域 $\mathbf{Q}$ 上椭圆曲线：

$$E: y^2=x^3+17$$

以及其上的点：

$$P_1=(-2,3),P_2=(-1,4),P_3=(2,5),P_4=(4,9),P_5=(8,23)$$

(1) 试验证：$P_5=-2P_1,P_4=P_1-P_3$ ；

(2) 计算：$2P_2,P_2+P_3$ 。

B 组

2. 给定 1 中椭圆曲线上点：$P_6=(43,282),P_7=(52,375)$，试用 P_1,P_3 生成 P_6,P_7，即将 P_6,P_7 表示为 mP_1+nP_3。

3．给定复数域 $\mathbf{C}$ 上的椭圆曲线 E，证明：$E(\mathbf{C})$ 是不可数的。

9.5 有限域上的椭圆曲线

上一节中给出了任意特征不为 2、3 的域上椭圆曲线为 Mordel-Weil 群的运算公式，本节将重点介绍有限域 F_{p^n}（$p>3$且为素数）上，特别是 $\mathbf{Z}_p$（$p>3$且为素数）和 F_{2^m} $(m\geq 1)$ 上的椭

圆曲线。

F_{p^n} 上的椭圆曲线加法定义与定理 9.4.3 一致，只是需要注意当 $n \geq 2$ 时，F_{p^n} 中的加法、乘法、加法逆元、乘法逆元的求法比域 $\mathbf{Z}_p$ 的模 p 运算更加复杂（参七章 4 节、八章 5 节），我们这里就不在赘述其上椭圆曲线的例子，而是直接介绍 $\mathbf{Z}_p(p>3$且为素数$)$ 上的椭圆曲线。

定义 9.5.1 设 $\mathbf{Z}_p(p>3$且为素数$)$ 为特征大于 3 的素域，则 $\mathbf{Z}_p$ 上椭圆曲线 $E(\mathbf{Z}_p)$ 有类似于式(9.3.1)的形式，为简单起见，在密码学实践中，将 $E(\mathbf{Z}_p)$ 的 Weierstrass 方程定义为

$$E(\mathbf{Z}_p): y^2 = x^3 + ax + b \quad , \tag{9.5.1}$$

其中 $\Delta = -16(4a^3 + 27b^2) \neq 0$．有些文献将特征大于 3 的素域 $\mathbf{Z}_p$ 上的椭圆曲线方程记为

$$E: y^2 \equiv x^3 + ax + b \pmod{p} \quad , \tag{9.5.1'}$$

简记为 $E_p(a,b)$.

将方程(9.5.1)与标准 Weierstrass 方程(9.3.1)相比较，我们得到

$$a_1 = a_2 = a_3 = 0, \quad a_4 = a, \quad a_6 = b ,$$

由此可导出椭圆曲线 $E(\mathbf{Z}_p)$ 上点的负元公式和加法公式.

设 $P_1 = (x_1, y_1)$， $P_2 = (x_2, y_2)$ 是 $E(\mathbf{Z}_p)$ 上的异于无穷远点 O 的两个点，由式(9.4.3)可得

$$-P_1 = (x_1, -y_1 - a_1x_1 - a_3) = (x_1, -y_1) \quad , \tag{9.5.2}$$

如果 $P_2 = -P_1$，则 $P_1 + P_2 = O$；如果 $P_2 \neq -P_1$，设 $P_3 = (x_3, y_3) = P_1 + P_2$，由式(9.2.18)可得

$$\begin{cases} x_3 = k^2 + a_1k - a_2 - x_1 - x_2 = k^2 - x_1 - x_2 \\ y_3 = k(x_1 - x_3) - a_1x_3 - y_1 - a_3 = k(x_1 - x_3) - y_1 \end{cases} \tag{9.5.3}$$

其中参数 k 定义为

$$k = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \quad , & \text{如果} x_1 \neq x_2 \text{(对应于点加)} \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} = \dfrac{3x_1^2 + a}{2y_1} \quad , & \text{如果} x_1 = x_2 \text{(对应于倍加)} \end{cases} \tag{9.5.4}$$

例 9.5.1 求 $\mathbf{Z}_5$ 上椭圆曲线

$$E: y^2 \equiv x^3 + 2x + 3 \pmod 5$$

上的所有点（即所有关于 $\mathbf{Z}_5$ 的有理点），并在其中选两个点计算它们的加法.

解　x (mod 的所有可能值为 0，1，2，3，4. 将它们代入 E 的方程可以计算出相应 y 的值，从而得到 E 上点的坐标，计算过程如表 9.2.2 所示.

表 9.5.1　例 9.5.1 计算过程

$x \equiv 0$	$y^2 \equiv 3 \pmod 5$	y 无解
$x \equiv 1$	$y^2 \equiv 6 \equiv 1 \pmod 5$	$y \equiv 1, 4 \pmod 5$
$x \equiv 2$	$y^2 \equiv 15 \equiv 0 \pmod 5$	$y \equiv 0 \pmod 5$
$x \equiv 3$	$y^2 \equiv 36 \equiv 1 \pmod 5$	$y \equiv 1, 4 \pmod 5$
$x \equiv 4$	$y^2 \equiv 75 \equiv 0 \pmod 5$	$y \equiv 0 \pmod 5$

所以椭圆曲线 $E: y^2 \equiv x^3 + 2x + 3 \pmod 5$ 上所有点为：

$$(1, 1),\ (1, 4),\ (2, 0),\ (3, 1),\ (3, 4),\ (4, 0),\ O.$$

下面我们在 $E: y^2 \equiv x^3 + 2x + 3 \pmod 5$ 上计算(1, 4) + (3, 1).

$$k \equiv \frac{y_2 - y_1}{x_2 - x_1} \equiv \frac{1-4}{3-1} \equiv 1 \pmod 5,$$

$$\begin{cases} x_3 \equiv k^2 - x_1 - x_2 \equiv 1^2 - 1 - 3 \equiv 2 \pmod 5 \\ y_3 \equiv k(x_1 - x_3) - y_1 \equiv 1(1-2) - 4 \equiv 0 \pmod 5 \end{cases}$$

所以

$$(1, 4) + (3, 1) = (2, 0).$$

定义 9.5.2　椭圆曲线 $E(K)$ 上点的个数称为**椭圆曲线 $E(K)$ 的阶**，记为 $\#E(K)$. 设 P 是椭圆曲线 $E(K)$ 上的一点，若存在最小的整数 n，使得 $nP = O$，则称 n 是**点 P 的阶**，记作

$$\text{ord}\, P = n.$$

如果椭圆曲线 $E(K)$ 上点 P 的阶存在，由群论中的拉格朗日定理知 $\text{ord}\, P \mid \#E(K)$.

事实上，有限域上的椭圆曲线上所有的点 P 的阶都是存在的（证明从略）.

由例 9.5.1 可知椭圆曲线 $E: y^2 \equiv x^3 + 2x + 3 \pmod 5$ 的阶为 7. 一般地，对于椭圆曲线 $E(\mathbf{Z}_p)$，因为 $\mathbf{Z}_p$ 中共有 p 个元素，根据 Weierstrass 方程 $y^2 = x^3 + ax + b$ 可知 $\#E(K) \leqslant 2p + 1$（加 1 是因为有无穷远点），

更进一步，我们有 Hass 定理[9,11]：

定理 9.5.1 (Hass **定理**) 设 E 是定义在 $\mathbf{Z}_q(q=p^n, p$是素数$)$ 上的椭圆曲线，则 E 的阶 $\#E(\mathbf{Z}_p)$ 满足

$$\left|\#E(\mathbf{Z}_q)-(q+1)\right| \leqslant 2\sqrt{q} \tag{9.5.5}$$

由 Hass 定理知，当 q 足够大时，$\#E(\mathbf{Z}_p)$ 近似等于 q.

例 9.5.2 求椭圆曲线 $E_{23}(1,1)$ 的上所有的点，并画出其图像.

解 $E_{23}(1,1)$ 的方程为 $y^2 = x^3 + x + 1 \pmod{23}$，表 9.2.3 列出了曲线上的所有点.

表 9.5.2 例 9.5.2 的所有点

(0, 1)	(6, 4)	(12, 19)
(0, 22)	(6, 19)	(13, 7)
(1, 7)	(7, 11)	(13, 16)
(1, 16)	(7, 12)	(17, 3)
(3, 10)	(9, 7)	(17, 20)
(3, 13)	(9, 16)	(18, 3)
(4, 0)	(11, 3)	(18, 20)
(5, 4)	(11, 20)	(19, 5)
(5, 19)	(12, 4)	(19, 18)

将表9.5.2中的点画在平面直角坐标系中，我们得到椭圆曲线 $E_{23}(1,1)$ 的图像，如图9.5.1所示.

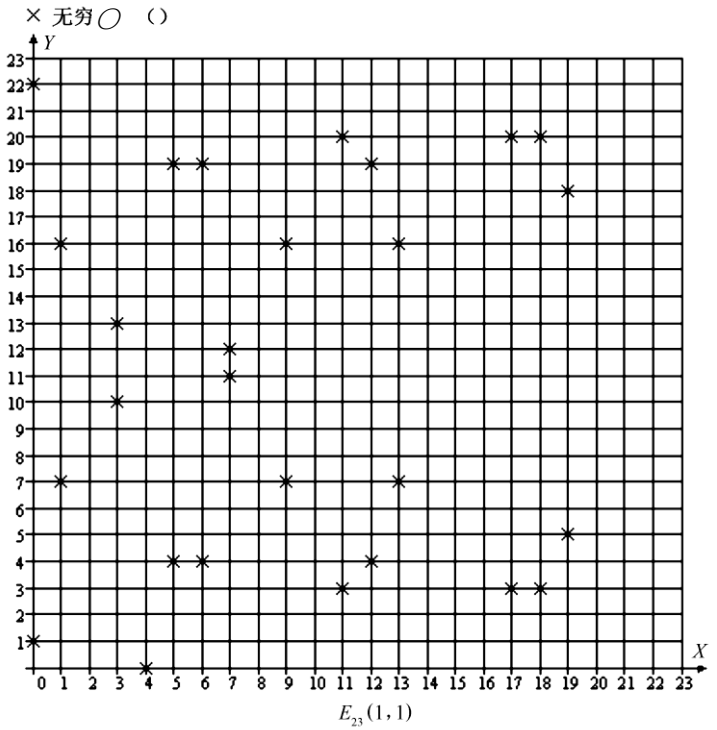

图 9.5.1　椭圆曲线 $E_{23}(1,1)$ 的图像

从图上可以看出，有限域上的椭圆曲线并不是一条连续的“曲线”，而是一系列离散的点，于是，前面定义椭圆曲线上点的加法时用到的“切线”、“斜率”等概念就不像对实数域上的椭圆曲线那样有明确的几何意义，只能从抽象的角度来理解.

从这个例题还可以看出，椭圆曲线 $E_{23}(1,1)$ 上共有 28 个点（加上无穷远点 O），因此我们有

$$\#E_{23}(1,1) = 28.$$

对于 p 较大时，求椭圆曲线 $E_p(a,b)$ 的阶是一件计算量很大的事情，如何快速有效地计算一条随机选取的椭圆曲线的阶是椭圆曲线理论中的一个有重要实用意义的问题，感兴趣的读者可参考有关资料.

例 9.5.3　已知 $P = (1, 3)$ 为 $\mathbf{Z}_{2773}$ 上椭圆曲线

$$E: y^2 \equiv x^3 + 4x + 4 \pmod{2\,773}$$

上的点，求 $2P$.

解　由广义欧几里得除法可知 $2\,311 \times 6 \equiv 1 \pmod{2\,773}$，所以

$$k \equiv \frac{3x_1^2 + a}{2y_1} \equiv \frac{3 \cdot 1^2 + 4}{2 \cdot 3} \equiv \frac{7}{6} \equiv 7 \times 2\,311 \equiv 2\,312 \pmod{2\,773},$$

$$\begin{cases} x_3 \equiv k^2 - x_1 - x_2 \equiv 2\,312^2 - 1 - 1 \equiv 1\,771 \pmod{2\,773} \\ y_3 \equiv k(x_1 - x_3) - y_1 \equiv 2\,312(1 - 1\,771) - 3 \equiv 705 \pmod{2\,773} \end{cases}$$

所以有　　$2P = P + P = (1\,771,\ 705).$

设域 K 的特征为 2，$E(K)$ 是定义在 K 上的椭圆曲线

$$E(K): y^2 + \bar{a}_1 xy + \bar{a}_3 = x^3 + \bar{a}_2 x^2 + \bar{a}_4 x + \bar{a}_6,$$

由式(9.3.8)知

$$j(E(k)) = (\bar{a}_1)^{12} / \Delta.$$

当 $j(E(k)) \neq 0$，即 $\bar{a}_1 \neq 0$ 时，作坐标变换

$$\begin{cases} x = (\bar{a}_1)^2 x + \dfrac{\bar{a}_3}{\bar{a}_1} \\ y = (\bar{a}_1)^3 y + \dfrac{(\bar{a}_1)^2 \bar{a}_4 + (\bar{a}_1)^2}{(\bar{a}_1)^3} \end{cases}$$

$E(K)$ 可化为

$$y^2 + xy = x^3 + ax^2 + b.$$

最后我们介绍密码学中常用的 F_{2^m} 上的椭圆曲线

定义 9.5.3 在密码学实践中，F_{2^m} 上椭圆曲线 $E(F_{2^m})$ 的 Weierstrass 方程定义为

$$E(F_{2^m}): y^2 + xy = x^3 + ax^2 + b, \tag{9.5.6}$$

其中 $b \neq 0$，这是因为式(9.5.6)给出的 Weierstrass 方程 $\Delta = b$（请读者自己验证）. 特别地，当 $a=0,\ b=1$ 或 $a=1,\ b=1$ 时，式(9.5.6)称为 **Koblitz 曲线**，常记作 K–m，此类曲线在实现椭圆曲线密码体制时速度较快.

$E(F_{2^m})$

与 $E(\mathbf{Z}_p)$ 上类似，我们可以导出 $E(F_{2^m})$ 上点的负元公式和加法公式.

设 $P_1=(x_1,y_1)$，$P_2=(x_2,y_2)$ 是 $E(\mathrm{F}_{2^m})$ 上的异于无穷远点 O 的两个点，则

$$-P_1=(x_1,-y_1-x_1)=(x_1,x_1+y_1), \tag{9.5.7}$$

如果 $P_2=-P_1$，则 $P_1+P_2=O$；如果 $P_2\neq -P_1$，设 $P_3=(x_3,y_3)=P_1+P_2$，则

$$\begin{cases} x_3 = k^2 + a_1k - a_2 - x_1 - x_2 = k^2 + k + a_2 + x_1 + x_2 \\ y_3 = k(x_1 - x_3) - a_1x_3 - y_1 - a_3 = k(x_1 + x_3) + x_3 + y_1 \end{cases} \tag{9.5.8}$$

其中参数 k 定义为

$$k=\begin{cases} \dfrac{y_2-y_1}{x_2-x_1}=\dfrac{y_2+y_1}{x_2+x_1}, & \text{如果} x_1\neq x_2 \text{(对应于点加)} \\ \dfrac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}=\dfrac{x_1^2+y_1}{x_1}, & \text{如果} x_1=x_2 \text{(对应于倍加)} \end{cases} \tag{9.5.9}$$

例 9.5.4 以 $\mathbf{Z}_2$ 上不可约多项式 $f(t)=t^2+t+1$ 为本原多项式，我们可以得到有限域 F_{2^2} 的一种表示形式，

即

$$\mathrm{F}_{2^2}=\{0,1,t,1+t\}(\bmod f(t)),$$

据此求椭圆曲线 $E(F_{2^2}): y^2+xy=x^3+ax^2+t$ 上的所有点.

解 $x\equiv 0 \pmod{f(t)} \Rightarrow y^2\equiv t \pmod{f(t)} \neq 1+t \pmod{f(t)}$，

$x\equiv 1 \pmod{f(t)} \Rightarrow y^2+y\equiv 1+t \pmod{f(t)} \Rightarrow y$ 无解，

$x\equiv t \pmod{f(t)} \Rightarrow y^2+ty\equiv t^3+t\equiv t+1 \pmod{f(t)} \Rightarrow y\equiv 1,1+t \pmod{f(t)}$，

$x\equiv t+1 \pmod{f(t)} \Rightarrow y^2+(t+1)y\equiv t^3+t\equiv 1 \pmod{f(t)} \Rightarrow y$ 无解，

所以 $E(F_{2^2}): y^2+xy=x^3+ax^2+t$ 上的所有点为

$$(0,1+t),\ (t,1),\ (t,1+t),\ O.$$

习题 9.5

A 组

1. 求 $E_{17}(1, 1)$上的所有点，并求这些点的阶.

2. 已知 $E_{11}(1, 6)$上一点 $G(2, 7)$，求 $2G$ 到 $13G$ 所有的值.

B 组

3. 设素数 $p>3$，有限域 Z_p 上的椭圆曲线 E：$y^2 \equiv x^3 + ax + b \pmod p$，$a,b \in \mathbf{Z}_p$ 且 $4a^3 + 27b^2 \neq 0$。

(1)证明：$|E| \leq 2p+1$。

(2)若在 Z_{11} 上定义椭圆曲线 $E: y^2 = x^3 + x + 6$，点 $P = (5, y) \in E$ 且 $0 \leq y \leq 6$，求 y 以及点 $3P$ 的坐标。

4.设 $\mathbf{Z}_{17}$ 上的椭圆曲线

$$E: y^2 = x^3 + 3x + 1,$$

以及其上的两点 $P = (7,5)$，$Q = (15,2)$，

（1） 求 P 在群 $(E,+)$ 中的阶。

（2） 求 Q 在群 $(E,+)$ 中的阶。

（3） 设已由 Hasse 定理知，E 的阶 $|E|$ 满足：

$$||E| - (q+1)| \leq 2\sqrt{q}$$

试根据（1）（2）确定 E 的阶 $|E|$。

5. 求 F_{7^2} 上的椭圆曲线 $E: y^2 = x^3 + 3x + 1$ 上任一点（非无穷远点），并求该点的阶。

附 椭圆曲线上的离散对数

椭圆曲线上的离散对数是循环群上的离散对数的一种特例. 给定有限域 F_q（$q = p^r$ 为素数幂）上的一条椭圆曲线 E，并给定这条曲线上的两点 P 和 Q，求正整数 k（如果存在的话）使之满足 $Q = kP$ 的问题，称为椭圆曲线上的离散对数问题(ECDLP). 当点 P 的阶为大素数时，普遍认为 ECDLP 是难解的. 反过来，由第 9 章的知识，已知 E 上的一点 P 和正整数 k，求 E 上的另一点 $Q = kP$ 则是很容易的.

与一般的离散对数问题一样，穷举法、商克法、Pollard's ρ算法也适用于椭圆曲线上的离散对数问题. 下面举一个例子:

例 9.6.1 研究椭圆曲线 $E: y^2 = x^3 + 8x + 8 \pmod{19}$上的离散对数问题，已知$|E| = 13$, $P = (6, 14)$, $Q = (9, 7)$是 E 上的点，用 Pollard's ρ算法求正整数 k 使之满足 $Q = kP$.

解 设$T_i \equiv a_i P + b_i Q$，其中 a_i, b_i为整数, $a_0 = b_0 = 1$，$T_0 = P+Q = (1, 6)$，令 x_{T_i} 表示 T_i 的横坐标. 采用以下伪随机策略改变 a_i 和 b_i 的值:

- 如果 $x_{T_{i-1}} \pmod 3 = 0$，$a_i = 2a_{i-1} \pmod{|E|}$ ，$b_i = 2b_{i-1} \pmod{|E|}$
- 如果 $x_{T_{i-1}} \pmod 3 = 1$，$a_i = a_{i-1}+1 \pmod{|E|}$ ，$b_i = b_{i-1}$
- 如果 $x_{T_{i-1}} \pmod 3 = 2$，$a_i = a_{i-1}$，$b_i = b_{i-1}+1 \pmod{|E|}$
- 列表计算如下:

i	0	1	2	3	4
$a_iP + b_iQ$	$P+Q$	$2P+Q$	$3P+Q$	$4P+Q$	$8P+2Q$
T_i	(1, 6)	(10, 10)	(4,3)	(6,5)	(4,3)

所以, $3P+Q = 8P+2Q$, $5P + Q = O$, $Q = -5P = 8P$, $k = 8$.

习题 9.6

A 组:

1. 研究椭圆曲线 $E: y^2 = x^3 + 4x + 4 \pmod{11}$上的离散对数问题，已知$|E| = 11$, $P = (2, 8)$, $Q = (8, 3)$是 E 上的点，用穷举法和 Pollard's ρ算法求正整数 k 使之满足 $Q = kP$.
2. 研究椭圆曲线 $E: y^2 = x^3 + 4x + 2 \pmod{13}$上的离散对数问题，已知$|E| = 13$, $P = (4, 11)$, $Q = (7, 3)$是 E 上的点，用穷举法和 Pollard's ρ算法求正整数 k 使之满足 $Q = kP$.

B 组:

3. 研究椭圆曲线 $E: y^2 = x^3 + 4x + 13 \pmod{83}$上的离散对数问题，已知$|E| = 73$, $P =(19,68)$, $Q = (74, 24)$是 E 上的点，用穷举法和 Pollard's ρ算法求正整数 k 使之满足 $Q = kP$.