大学代数几何

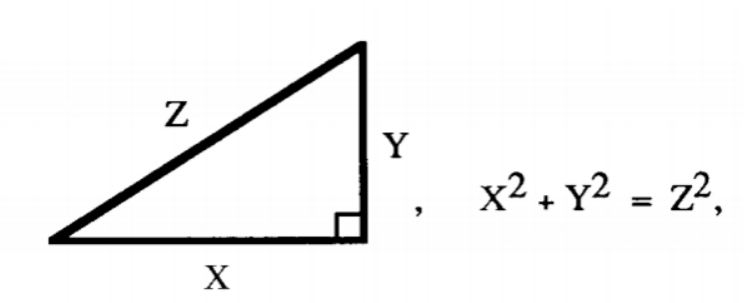
2020 年 2 月 4 日

Chapter 1

平面圆锥曲线

1.1 一个参数化曲线的例子

毕达哥拉斯的理论图解：



显然有 $(3,4,5)$ 与 $(5,12,13)$ 等解. 如何找全部整数解？等式 $X^2+Y^2=Z^2$ 是齐次的, 所以 $x=X/Z, y=Y/Z$ 就给出了圆 C $(X^2+Y^2=1)\supset R^2$, 它可以被参数化表示为：

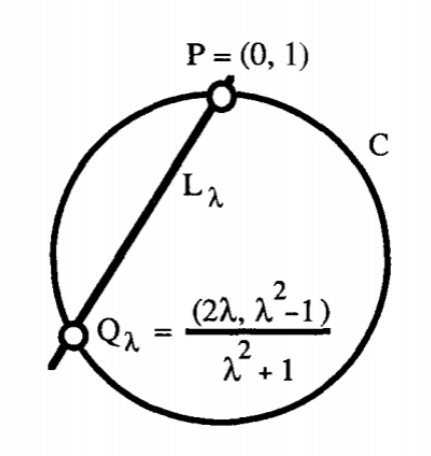
$$x=2\lambda/\left(\lambda^2+1\right), y=\left(\lambda^2-1\right)/\left(\lambda^2+1\right),\ \ \lambda=x/(1-y)$$

所以下式可以给出所有解：

$$X=2\ell m, Y=\ell^2-m^2, Z=\ell^2+m^2 \text{ 其中}\ell, m\in\mathbb{Z} \text{ 互素}$$

(若 ℓ, m 都是奇数, 得到的 X, Y, Z 值也可以各除以 2). 由于该等式为齐次, 所以如果 (X, Y, Z) 是一组解, 那么 $(\lambda X, \lambda Y, \lambda Z)$ 也是一组解.

在之前的几何教学中, 我们已经对参数化有了相当的了解, 并且通常我们都能很简单地判断参数化是否有效. 而如果我们不是很了解参数化, 我们可以通过下面的从定点出发的线性映射来初步地理解：



$P = (0,1) \in C$, 如果 $\lambda \in Q$ 取任意值, 那么穿过 P 点斜率为 $-\lambda$ 的直线 L_λ 与 C 相交于另一点 Q_λ. 这种线性映射的映射结构会在以后的讨论中经常出现.

1.2 相似的例子

对于 $C : (2X^2 + Y^2 = 5Z^2)$ 我们可以构造一个 $\mathbb{Z} \to C$ 的参数化的映射：

$$x = \frac{2\sqrt{5}\lambda}{1+2\lambda^2}, \quad y = \frac{2\lambda^2 - 1}{1+2\lambda^2}$$

这样有助于我们理解 C 上所有实系数的点, 而且和之前的例子没有本质上的区别. 那么, 如果是有理系数呢？

命题 如果 $(a,b,c) \in \mathbb{Q}$ 满足 $2a^2 + b^2 = 5c^2$ 那么 $(a,b,c) = (0,0,0)$.

证明 通过同时乘公分母与除以公因子, 可以使得 a, b, c 为整数, 且他们不能同时为 5 的倍数. 而如果 $5|a$ 且 $5|b$ 那么 $25|c$, 即 $5|c$, 这与上述题设矛盾. 考虑 a 和 b 除以 5 的余数很容易得到矛盾：任何数的平方除以 5 后的余数只可能为 0,1 或 4, 即 $2a^2 + b^2$ 除以 5 的余数只能是 0+1,0+4,2+0,2+1,2+4,8+0,8+1 以及 8+4 中的一个, 而这些都不能写成 $5c^2$ 的形式.

注意, 这是一个完整的算数证明.

1.3 $\mathbb{Q}^2$ 中的圆锥曲线

$\mathbb{Q}^2$ 中的圆锥曲线是由二次方程 $q(x,y) = ax^2 + bxy + cy^2 + dx + ey + f = 0$ 给出的平面曲线.

非退化的曲线有以下三种分类:

1. 椭圆 $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$　　2. 抛物线 $y = mx^2$　　3. 双曲线 $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$

此外, 还有一些特殊情况：

4. 由 $x^2 + y^2 = 0$ 给出的单点.

5.6.7. 为三种类型方程给出的空集：$5.x^2 + y^2 = -1$　　$6.x^2 = -1$　　$7.0 = 1.$

虽然这三种类型的方程都表示 R^2 上的空集, 但是它们是不同的——例如考虑它们的复数解.

8. 一条直线:$x = 0$.

9. 一对相交直线:$xy = 0$.

10. 一对平行直线:$x(x-1) = 0$.

11. 重合的直线:$x^2 = 0$.

12. 整个平面：$0 = 0$.

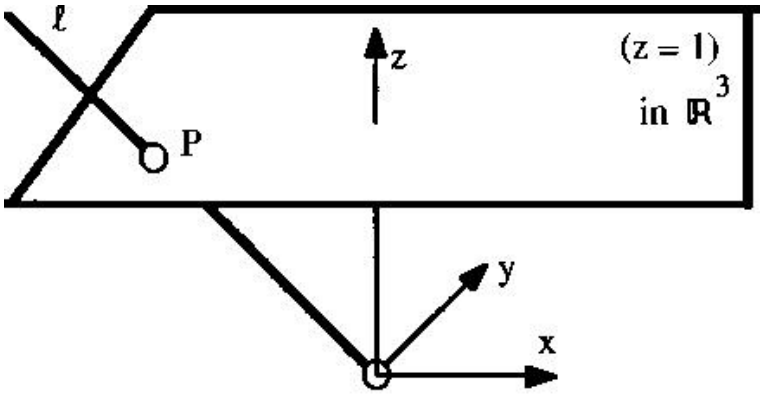
1.4 射影平面 $\mathbb{P}^2_{\mathbb{R}}$

定义

$$\begin{aligned}\mathbb{P}^2_{\mathbb{R}} &= \mathbb{R}^3\text{中过原点的直线}\\ &= \{\text{比例}X:Y:Z\}\\ &= \left(\mathbb{R}^3\backslash\{0\}\right)/\sim,\ \text{其中}(X,Y,Z)\sim(\lambda X,\lambda Y,\lambda Z),\lambda\in\mathbb{R}\backslash\{0\}\end{aligned}$$

(这里可以将 $\mathbb{R}^3$ 推广到任意维的向量空间上)

为了表示 $Z \neq 0$ 时的比例 $X:Y:Z$, 可以设 $x = \dfrac{X}{Z}, y = \dfrac{Y}{Z}$, 这样比例就相当于两个实数. 换句话说, 等价类 $(X:Y:Z)$ 有一个特殊的代表元 $(x:y:1)$. 可是, 在 $Z=0$ 时, 选择这种代表元的方式就无法实现了. 这个讨论意味着 $\mathbb{P}^2_{\mathbb{R}}$ 包含着一个 $\mathbb{R}^2$, 如图：



$$\mathbb{R}^2 \hookrightarrow \mathbb{R}^3 \setminus \{0\} \to \mathbb{P}^2\mathbb{R} \text{ by } (x,\ y) \mapsto (x,\ y,\ 1)$$

$\mathbb{R}^2 \hookrightarrow \mathbb{R}^3\backslash\{0\} \to \mathbb{P}^2_{\mathbb{R}}$由$(x,y) \mapsto (x,y,1)$定义

$\mathbb{R}^3$ 中通过 0 且不包含在平面 $(Z=0)$ 的直线都与平面 $(Z=1)$ 交于一点, 这一点可以看做是等价类的代表元. 而包含在平面 $(Z=0)$ 中的直线与平面 $(Z=1)$ 无交点, 所以他们不对应于 $\mathbb{R}^2$ 中的点但对应于一个渐进方向, 或者说对应于,$\mathbb{R}^2$ 中的一组平行线. 所以可以认为 $\mathbb{P}^2_{\mathbb{R}}$ 是由 $\mathbb{R}^2$ 和每组平行线方向上的无穷远点组成的. 从这个角度来看, 可以在 $\mathbb{R}^2$ 中进行计算, 通过某种渐进理论去猜想在无穷远点的情况, 然后 (如果必要的话), 用齐次坐标去证明猜想. 从 $\mathbb{R}^3$ 中的直线来定义使之变得合理, 因为这个定义平等地对待 $\mathbb{P}^2_{\mathbb{R}}$ 上的所有点.

变换群在整个几何中都是非常重要的, 几何图形的性质要在一些变化类下保持不变才有意义.$\mathbb{R}^2$ 坐标中的仿射变换形式为 $T(x) = Ax + B$, 其中 $x = (x, y) \in \mathbb{R}^2$, 并且 A 是一个 2×2 的可逆矩阵,B 是一个平移向量；如果矩阵 A 是正交矩阵, 那么变换 T 为欧式变换. 每个非退化的曲线都可以通过欧式变换化成以上 (1-3) 的形式.

$\mathbb{R}^2_{\mathbb{R}}$ 中的射影变化形式为 $T(x) = MX$, 其中 M 是一个 3×3 的可逆矩阵. 很容易理解这个变换在仿射片 $\mathbb{R}^2 \subset \mathbb{P}^2_{\mathbb{R}}$ 上的影响：作为一代部分定义的映射 $\mathbb{R}^2 \to \mathbb{R}^2$, 这是一个分式线性变换

$$\begin{pmatrix} x \\ y \end{pmatrix} \to (A \begin{pmatrix} x \\ y \end{pmatrix} + B)/(cx + dy + e)$$

其中,

$$M = \begin{pmatrix} A & B \\ cd & e \end{pmatrix}$$

当 $cx + dy + e = 0$ 时, 这个变换无定义.

1.5 平面曲线的方程

非齐次二次多项式

$$q(x, y) = ax^2 + bxy + cy^2 + dx + ey + f$$

对应齐次二次方程式

$$Q(X, Y, Z) = aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2$$

这种对应关系很容易理解为菜谱, 或者你可以把它看作是由以下方面给出的双射 $Q \longleftrightarrow q$,

$$q(x, y) = Q(X/Z, Y/Z, 1)\text{其中}x = X/Z, y = Y/Z, Z = 1$$

反过来

$$Q = Z^2 q(X/Z, Y/Z)$$

平面曲线 $C \subset \mathbb{P}^2$ 是由 $C : (Q(X, Y, Z) = 0)$ 给出的曲线, 其中 Q 是齐次二次表达式; 条件 $Q(X, Y, Z) = 0$ 在等价类上是良定义的, 因为对任意的 $\lambda \in \mathbb{R}, Q(\lambda X) = \lambda^2 Q(X)$.

‘无穷远直线’与渐近方向 $\mathbb{P}^2$ 中 $Z = 0$ 表示的点对应比例 $(X : Y : 0)$, 这些点形成了‘无穷远直线’ $\mathbb{P}^1_{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$(因为 $(X : Y) \mapsto X/Y$ 定义了一个双射 $P^1_R \to R \cup \{\infty\}$)

$\mathbb{P}^2$ 中的直线是由 $L : (aX + bY + cZ = 0)$ 定义的, 并且 L 通过 $(X, Y, 0) \Longleftrightarrow aX + bY = 0$. 在仿射坐标中, 相同的直线是由 $ax + by + c = 0$ 给出的, 从而使所有 $a : b$ 比率相同的直线在无穷远处通过同一点. 这就是所谓的“平行线在无穷远处相遇”.

例子:

(a) $\mathbb{R}^2$ 中的双曲线 $(\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1)$ 对应于 $\mathbb{P}^2_{\mathbb{R}}$ 中的 C:$(\frac{X^2}{a^2} - \frac{Y^2}{b^2} = Z^2)$; 很明显, 在 $(b, \pm a, 0) \in \mathbb{P}^2_{\mathbb{R}}$ 的两点满足 $(Z = 0)$, 这两个点对应于双曲线的渐近线.

注意, 在 $\mathbb{P}^2_{\mathbb{R}}$ 的仿射片 $(X \neq 0)$ 中, 仿射坐标是 $u = Y/X, v = Z/X$, 这样 C 就变成了椭圆 $(\frac{u^2}{b^2} + v^2 = \frac{1}{a^2})$.

(b) $\mathbb{R}^2$ 中的抛物线 $(y = mx^2)$ 对应于 $\mathbb{P}^2_{\mathbb{R}}$ 中的 $C : (YZ = mX^2)$; 在单点 $(0, 1, 0)$ 处满足 $Z = 0$. 因此在 $\mathbb{P}^2$ 中, "抛物线的两个分支在无穷远处相遇".

1.6 $\mathbb{P}^2$ 中平面曲线的分类

k 是一个特征不为 2 的域, 回想二次型线性代数的两个结果:

命题 (A) 有天然的双射 {二次齐次多项式} = {二次型$k^3 \to k$} $\longleftrightarrow$ {k^3上的对称双线性型}, 并且可以由下式给出:

$$aX^2 + 2bXY + cY^2 + 2dXZ + 2eYZ + fZ^2 \longleftrightarrow \begin{bmatrix} a & b & d \\ b & c & e \\ d & e & f \end{bmatrix}$$

如果相应的双线性形式是非退化的, 则二次型是非退化的, 就是说, 这个矩阵是非奇异的.

定理 (B) V 是 k 上的向量空间,$Q : V \to k$是二次型, 则存在一组V的基使$Q = \varepsilon_1 x_1^2 + \varepsilon_2 x_2^2 + \cdots \varepsilon_n x_n^2$, 其中 $\varepsilon_i \in k$.(格拉姆-施密特正交化证明了这一点)

推论 在适当的坐标系中,$\mathbb{P}^2_{\mathbb{R}}$ 中的任何圆锥曲线都是下列情况之一:

(1) 非退化曲线, $C : (X^2 + Y^2 - Z^2 = 0)$;

(2) 空集, $(X^2 + Y^2 + Z^2 = 0)$;

(3) 交叉线对, $(X^2 - Y^2 = 0)$;

(4) 一个点 $(0, 0, 1)$, $(X^2 + Y^2 = 0)$;

(5) 重叠线 $(X^2 = 0)$;

(可以将 $\mathbb{P}^2_{\mathbb{R}}$ 整个平面由 $(0 = 0)$ 给出.)

证明 任何实数 ε 是 0 或 $\pm\sqrt{a}$, 因此我们只需要考虑定理中 $\varepsilon = 0$ 或 ± 1 的 Q. 另外, 由于我只对轨迹 $(Q = 0)$ 感兴趣, 所以我可以把 Q 乘以-1, 这将立即得出给定的列表.

关于这个推论有两点: 首先, 列表比 (1.3) 中的要短得多: 例如, (1.3) 的 3 个非退化情况 (椭圆、抛物线、双曲线) 都对应情况 (1). 在射影情形下不区分交叉和平行的线对这两种情况. 其次, 从一般代数学原理推导出以上几种情况更简单一点.

1.7 曲线参数化

设 C 是 $\mathbb{P}^2_{\mathbb{R}}$ 中的非退化的非空二次曲线. 由推论 1.6, 取新的坐标 $(X + Z, Y, Z - X)$, C 与曲线 $(XZ = Y^2)$ 在投影上等价, 这个曲线的参数化是

$$\begin{array}{ccc} \Phi : \mathbb{P}^1_{\mathbb{R}} & \longrightarrow & C \subset \mathbb{P}^2_{\mathbb{R}} \\ (U : V) & \longmapsto & (U^2 : UV : V^2) \end{array}$$

备注

1. 相反的映射 $\Psi : C \longrightarrow P^1_R$ 由 $(X : Y : Z) \longmapsto (X : Y) = (Y : Z)$ 给出; 如果 $Y \neq 0$, 就按左边的比例定义, 如果 $Z \neq 0$, 就按右边的比例定义. 在后面要介绍的术语中,Φ 和 Ψ 是变换的逆同构.

2. 任意非空的非退化二次曲线默认为投影等价于 $(XZ = Y^2)$; 在特征不为 2 的域中, 这在练习 5 中是合理的 (对特征为 2 的域感兴趣的读者应该把这个作为非退化二次曲线的定义).

1.8 2 个变量的齐次型

设 $F(U,V)$ 为关于 U,V 的 d 次非零齐次多项式, 系数在固定的域 k 内

$$F(U,V) = a_dU^d + a_{d-1}U^{d-1}V + ... + a_iU^iV^{d-i} + ...a_0V^d$$

F 有一个与之相关的单变量非齐次多项式:

$$f(u) = a_du^d + a_{d-1}u^{d-1} + ... + a_iu^i + ...a_0$$

显然对于 $\alpha \in k$, 有

$$f(\alpha) = 0 \Leftrightarrow (u-\alpha)|f(u) \Leftrightarrow (U-\alpha V)|F(U,V) \Leftrightarrow F(\alpha,1) = 0$$

所以 f 的零点对应于 F 在 $\mathbb{P}^1$ 上除点 $(1,0)$ 的零点, 而点 $(1,0)$ 对应于‘点 $\alpha = \infty$’.F 在无穷远处有一个零点是什么意思?

$$F(1,0) = 0 \Leftrightarrow a_d = 0 \Leftrightarrow degf < d$$

现在定义 F 在 $\mathbb{P}^1$ 上零点的重数为

(i) $\alpha \in k$ 在 f 中的重数;

(ii) 如果 $(1,0)$ 是零点, 重数为 $d - degf$.

所以 F 在 $(\alpha,1)$ 处的零点重数是 $(U-\alpha V)$ 除 F 的最大幂, 在 $(1,0)$ 处是 V 除 F 的最大幂.

命题 设 $F(U,V)$ 是 U,V 的 d 次的非零齐次多项式, 那么 F 在 $mathbbP^1$ 上最多有 d 个零点; 此外, 如果 k 是代数闭域, 那么 F 在 $mathbbP^1$ 上恰好有 d 个零点, 前提是这些数要用上面定义的乘法来计算.

证明 令 m_∞ 为 F 在 $(1,0)$ 处的零点重数; 然后根据定义, $d - m_\infty$ 是非齐次多项式 f 的次数, 然后这个命题可以归结为一个众所周知的事实, 即单变量多项式最多有 $degf$ 个根.

注意, 在代数封闭域上, F 将分解为线性形式 $\lambda_i = (a_iU + b_iV)$ 的乘积 $F = \Pi\lambda_i^{m_i}$, 用这种方法处理, 点 $(1,0)$ 对应于形式 $\lambda_\infty = V$, 并且与所有其他点处于相同的地位.

1.9 贝祖定理的简单情况

贝祖定理指出, 如果 C 和 D 是次数为 $degC = m, degD = n$ 的平面曲线, 并且

(i) 域是代数闭的;(ii) 交点个数按重数来计数;(iii) 我们在 $\mathbb{P}^2$ 中计算, 所以考虑无穷远处的交点. 则 C 和 D 的交点个数为 mn. 见 [Fulton,p.112] 有自成一体的证明. 在本节中, 将在其中一条曲线是直线或二次曲线的情况下证明.

定理 设 $L \subset \mathbb{P}_k^2$ 是一条直线 ($C \subset \mathbb{P}_k^2$ 是一条非退化二次曲线), $D \subset \mathbb{P}_k^2$ 是由 D : $(G_d(X,Y,Z) = 0)$ 定义的一条曲线, 其中 G 是关于 X,Y,Z 中的 d 次齐次多项式. 假定 L

不包含于 D(C 不包含于 D); 则 L 与 D 的交点个数 $\#\{L\cap D\}$ 小于等于 d ($\#\{C\cap D\}$ 小于等于 $2d$).

事实上, 对于交点的重数有一个自然的定义, 使得对于用重性计数的交点的个数, 不等式仍然成立, 如果 k 是代数闭的, 那么等式成立.

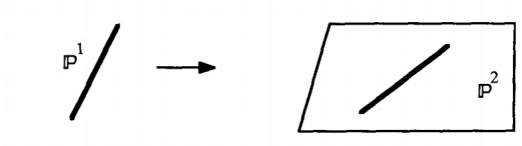
证明 λ 为线性形式, 由 $\lambda=0$ 给出的一条直线 $L\subset P_k^2$, 将其按下面方式参数化

$$X=a(U,V),Y=b(U,V),Z=c(U,V)$$

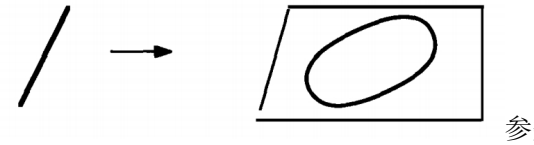
其中 a,b,c 是 U,V 的线性形式. 例如, 如果 $\lambda=\alpha X+\beta Y+\gamma Z$, 且 $\gamma\neq 0$, 那么 L 可以参数化为 $X=U,Y=V,Z=-\dfrac{\alpha}{\gamma}U-\dfrac{\beta}{\gamma}V$. 类似的, 正如 (1.7) 中证明的, 非退化曲线可以参数化为 $X=a(U,V),Y==b(U,V),Z=c(U,V)$. 其中 a,b,c 是 U,V 中的二次型, 这是因为 C 是 $(XZ=Y^2)$ 的射影变换, 它的参数化方式为 $(X,Y,Z)=(U^2,UV,v^2)$, 所以 C 是

$$\begin{bmatrix}X\\Y\\Z\end{bmatrix}=M\begin{bmatrix}U^2\\UV\\V^2\end{bmatrix}$$

其中 M 是 3×3 非奇异矩阵.



参数化直线


参数化二次曲线

然后通过 $F(U:V)=G_d(a(U,V),b(U,V),c(U,V))=0$ 求出 $(U:V)$ 的比值, 求出 L(或曲线 C) 与 D 的交点. 但 F 是关于 U,V 的 d(或为 $2d$) 次的齐次多项式, 因此可参考 (1.8) 得出结果.

1.10 推论

如果 $P_1,...,P_5\in\mathbb{P}_R^2$ 是任意四点不共线的 5 个点, 那么就至多存在一条圆锥曲线穿过 $P_1,...,P_5$.

证明用反证法假设 C_1 和 C_2 是两条不相同的圆锥曲线使得

$$C_1\cap C_2\supset\{P_1,...,P_5\}$$

C_1 是非空的因此它是非退化的, 那么, 由 (1.7), 它投影地等价于参数化的圆锥曲线

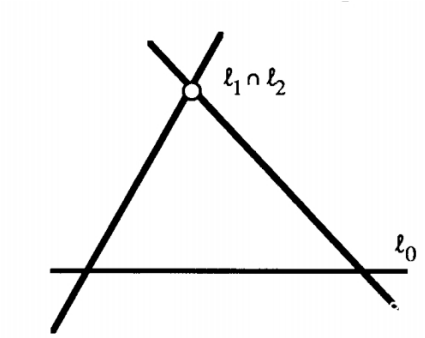
$$C_1=\{(U^2,UV,V^2)\mid(U,V)\in P^1\}$$

由 (1.9),$C_1 \subset C_2$. 那么, 如果 Q_2 与 C_2 相等, 那么 $Q_2(U^2, UV, V^2) \equiv 0$ 对于任何 $(U, V) \in P^1$ 成立, 并且通过简单计算 (如习题 1.6) 就可以看出 Q_2 是 $(XZ - Y^2)$ 的倍数, 这与 $C_1 \neq C_2$ 相矛盾.

现在假设 C_1 是退化的, 由 (1.6) 可知, 它是一组线对或是一条线, 而且很明显有

$$C_1 = L_0 \cup L_1, C_2 = L_0 \cup L_2$$

其中 $L_1 L_2$ 是不同的线. 那么 $C_1 \cap C_2 = L_0 \cup (L_1 \cap L_2)$



因此,$P_1 ... P_5$ 中的 4 点在 P_0 上, 自相矛盾.

1.11 所有二次曲线的空间

$S_2 = \{R^3$中的二次型$\} = \{3 \times 3$对称矩阵$\} \cong R^6$, 如果 $Q \in S_2, Q = aX^2 + 2bXY + \cdots fZ^2$; 对于 $P_0 = (X_0, Y_0, Z_0) \in P_R^2$, 考虑到 $P_0 \in C : (Q = 0)$ 的关系, 这是形式 $Q(X_0, Y_0, Z_0) = aX_0^2 + 2bX_0Y_0 + \cdots fZ_0 = 0$, 对于固定的 P_0, 这是关于 $(a, b, \cdots f)$ 的线性方程. 所以 $S_2(P_0) = \{Q \in S_2 | Q(P_0) = 0\} \cong R^5 \subset S_2 = R^6$ 是一个 5 维的超平面.

对于 $P_1, \cdots P_n \in P_R^2$, 类似地定义 $S_2(P_1, \cdots P_n) = \{Q \in S_2 | Q(P_i) = 0 i = 1, \cdots n\}$; 所以可以得到关于 Q 的 6 个系数 $(a, b, \cdots f)$ 的 n 个线性方程. 这得出了以下结果:

命题 $dim S_2(P_1, \cdots P_n) \geq 6 - n$.

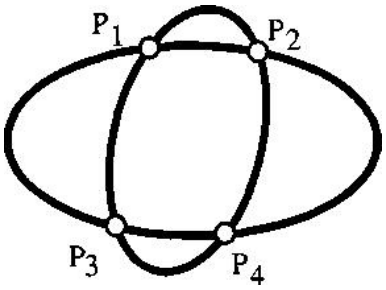
如果 $P_1, \cdots P_n$ 能都满足以些条件, 我们也可以期望等式成立, 更准确地说应该是:

推论 如果 $n \leq 5$ 并且 $P_1, \cdots P_n$ 中任意 4 点不共线, 则 $dim S_2(P_1, \cdots P_n) = 6 - n$.

证明 推论 1.10 表明, 如果 n = 5, $dim S_2(P_1, \cdots P_n) \leq 1$, 给出了这种情况的证明. 如果 $n \leq 4$, 然后我可以加入点 $P_{n+1}, \cdots, P_5$ 并且保持没有 4 个点共线的条件, 由于每个点最多增加一个线性条件, 所以 $1 = dim S_2(P_1, \cdots P_5) \geq dim S_2(P_1, \cdots P_n) - (5 - n)$.

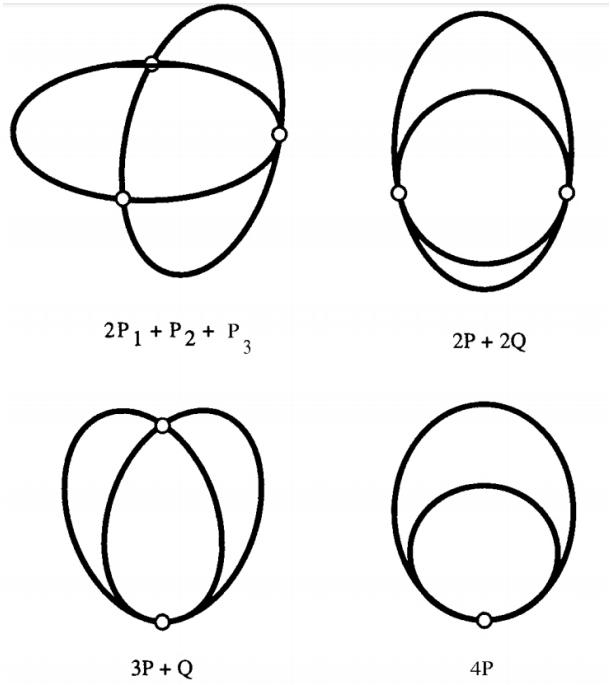
请注意, 如果给定 6 个点 $P_1, \cdots P_6$, 可能存在在一条圆锥曲线同时包含这 6 个点, 也可能不存在.

1.12 两条圆锥曲线的交点



正如我们上面所看到的, 两个二次曲线经常会在 4 个点相交; 相反, 根据推论 (1.11), 给定 4 个点 $P_1, \cdots P_4 \in P^2$, 在适当条件下 $S_2(P_1, \cdots P_4)$ 是一个二维向量空间, 因此选择 $S_2(P_1, \cdots P_4)$ 的一组基 Q_1, Q_2 给出了 2 条二次曲线 C_1, C_2, 使得 $C_1 \cap C2 = \{P^1, \cdots P^4\}$.

这里还有许多非退化曲线多重交点的可能性：



有关合适的方程式见练习 *1.9a*

1.13 退化的圆锥曲线族

定义 圆锥曲线族是一类满足以下特点的齐次多项式：

$$C_{(\lambda,\mu)} : (\lambda Q_1 + \mu Q_2 = 0)$$

其中的每一个元素都是一条由参数 (λ,μ) 线性控制的平面圆锥曲线. 类似于我们在 $\mathbb{P}^1$ 上做的那样, 我们可以用一个比例 $(\lambda:\mu)$ 来代表对应的平面圆锥曲线.

如示例中, 只有当 $(\lambda:\mu)$ 为一个特殊值时, 平面圆锥曲线 $C_{(\lambda,\mu)}$ 才是退化的. 事实上, 如果将二次齐次多项式 Q 对应的 3×3 对称矩阵的行列式记作 $\det(Q)$, 那么显然有

$$C_{(\lambda,\mu)}\text{是退化的} \iff \det\left(\lambda Q_1+\mu Q_2\right)=0$$

将对称矩阵 Q_1 和 Q_2 表述的条件记作：

$$F(\lambda,\mu)=\det\left|\lambda\begin{bmatrix} a & b & d\\ b & c & e\\ d & e & f\end{bmatrix}+\mu\begin{bmatrix} a' & b' & d'\\ b' & c' & e'\\ d' & e' & f'\end{bmatrix}\right|=0$$

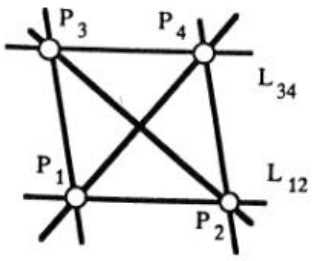
那么就可以注意到 $F(\lambda,\mu)$ 是一个对于 λ,μ 的三次齐次多项式, 那么我们就可以对 F 应用 (1.8) 的结论：

命题 假设 $C_{(\lambda,\mu)}$ 是在 $\mathbb{P}^2_k$ 上的一族圆锥曲线, 并且这一族圆锥曲线至少有一个非退化的 (因此 $F(\lambda,\mu)$ 不总是 0), 那么这一族中最多有三个退化的圆锥曲线. 另外, 如果有 $k=\mathbb{R}$, 那么这一族最少有一个退化的圆锥曲线.

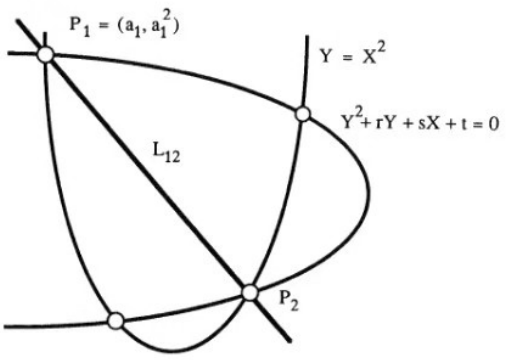
证明 一个三次齐次多项式的零点个数 ≤ 3. 而在 $\mathbb{R}$ 上, 它最少有一个零点.

1.14 一些实例

令 $P_1\ldots P_4$ 是 $\mathbb{P}^2_{\mathbb{R}}$ 上任意三个不共线的四点, 则经过这四点的圆锥曲线族 $C_{(\lambda,\mu)}$ 有三个退化的元素, 即线对 $L_{12}+L_{34}, L_{13}+L_{24}, L_{14}+L_{23}$, 其中 L_{ij} 是过 P_i,P_j 的直线：



然后, 我们假设这一族圆锥曲线是由 $Q_1=Y^2+rY+sX+t$ 和 $Q_2=Y-X^2$ 生成的, 并寻找 $P_1\ldots P_4$ 这四个交点.



通过下列步骤可解：

(1) 找出三个比例 $(\lambda:\mu)$ 使得 $C_{(\lambda,\mu)}$ 是退化的圆锥曲线. 根据上文, 这意味着我们需要找到三次齐次多项式的三个根

$$\begin{aligned} F(\lambda,\mu) &= \det\left|\lambda\begin{bmatrix} 0 & 0 & s/2 \\ 0 & 1 & r/2 \\ s/2 & r/2 & t \end{bmatrix} + \mu\begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 1/2 \\ 0 & 1/2 & 0 \end{bmatrix}\right| \\ &= -\frac{1}{4}\left(s^2\lambda^3 + \left(4t - r^2\right)\lambda^2\mu - 2r\lambda\mu^2 - \mu^3\right) \end{aligned}$$

(2) 从退化的圆锥曲线中分出 2 条作为线对 (这意味着解两个四次方程).

(3) 这四个交点 P_i 就是线的交点.

这个步骤给出了利用伽罗瓦理论解四次方程的一个几何解释：设 k 是一个域, 而 $f(X) = X^4 + rX^2 + sX + t \in k[X]$ 是一个四次多项式. 则两条抛物线 C_1 和 C_2 相交于四个点 $P_i = (a_i, a_i^2)\,(i = 1\ldots4)$, 而 a_i 是 f 的四个根.

则直线 $L_{ij} = P_iP_j$ 由下式给出：

$$L_{ij} : \left(Y = \left(a_i + a_j\right)X - a_ia_j\right)$$

而可约的圆锥曲线 $L_{12} + L_{34}$ 由下式给出：

$$Y^2 + \left(a_1a_2 + a_3a_4\right)Y + \left(a_1 + a_2\right)\left(a_3 + a_4\right)X^2 + sX + t = 0$$

这是由 $Q_1 - \left(a_1 + a_2\right)\left(a_3 + a_4\right)Q_2 = 0$ 推出的. 因此, 使圆锥曲线 $\lambda Q_1 + \mu Q_2$ 退化为线对的 3 个比例 $(\lambda:\mu)$ 的值为：

$$-\left(a_1 + a_2\right)\left(a_3 + a_4\right), -\left(a_1 + a_3\right)\left(a_2 + a_4\right), -\left(a_1 + a_4\right)\left(a_2 + a_3\right)$$

根是这三个数的三次方程被称为与四次方程对应的辅三次方程；这可以通过初等对称函数的理论计算得到；因此这是一个极具可操作性的步骤. 而在另一方面, 上面给出的概要优雅地给出了仅有三阶行列式的辅三次方程的一个推导.

练习 1

习题 1.1 考虑通过 $(-1,-2)$ 的直线, 将二次曲线 $C:(x^2+y^2=5)$ 参数化. 并找出 $(x^2+y^2=5)$ 的所有有理解.

解：由

$$\begin{cases} x^2+y^2=5 \\ y+2=k(x+1) \end{cases}$$

得

$$\begin{cases} x=\dfrac{-k^2+4k+1}{1+k^2} \\ y=\dfrac{2k^2+2k-2}{1+k^2} \end{cases}$$

若 (a,b) 是 $(x^2+y^2=5)$ 的解, 则 $(-a,-b),(-a,b),(a,-b)$ 也是 $(x^2+y^2=5)$ 的解. 所以不妨找 $a>0,b>0$ 的有理解, 由上述参数化知,(x,y) 是有理点 $\Leftrightarrow k\in Q$, $x>0,y>0\Leftrightarrow \frac{2}{\sqrt{5}+1}<k<\sqrt{5}+2$

习题 1.2 p 是质数, 猜想 $x^2+y^2=p$ 有有理解的充要条件, 证明你的猜想.

(若 $x^2=a(mod\ p)$ 有解, 称 a 是模 p 的二次剩余. 数论里的一个基本结论, -1 是模 p 的二次剩余当且仅当 $p=2$ 或 $p=1mod16$.)

解：猜想 $p=2$ 或 $p=1mod4$

$x^2+y^2=p$ 有有理解, $x=\frac{a}{c},y=\frac{b}{c},\Leftrightarrow a^2+b^2=pc^2$ 有整数解.

" $\Rightarrow$ " a 是模 p 的二次剩余 $\Leftrightarrow a^{\frac{p-1}{2}}=1(mod\ p)$, 显然 1 一定是模 p 的二次剩余 (因为 $a^{\frac{p-1}{2}}=1(mod\ p)$), 所以 $x^2=1(mod\ p)$ 有解. 若 (a,b,c) 满足 $a^2+b^2=pc^2$, 则一定满足 $a^2+b^2=pc^2(mod\ p)$. 因为一定存在 a, 使 $a^2=1(mod\ p)$, 所以一定存在 b 使 $b^2=-1(mod\ p)$, 得 $p=2$ 或 $p=1mod4$.

" $\Leftarrow$ " $p=2$ 时, $1^2+1^2=2$, 所以 $(1,1)$ 是 $x^2+y^2=2$ 的有理解.

$p=1mod4$ 时,$p=4k+1,k\in Z$ $a^2=1,0(mod4),b^2=1,0(mod4)$, 所以 $a^2+b^2=pc^2=1,2(mod4)$, 即 $a^2+b^2=pc^2=4k^2+1,4k^2+2$, 而 $pc^2=(4k+1)c^2=4kc^2+c^2=c^2(mod4)=1,2$,

习题 1.3 证明 1.3 中的陈述：仿射变换可以将任何一条圆锥曲线变为 1-12 中的形式.

解答：使用线性变换 $x\mapsto Ax$ 把 $ax^2+bxy+cy^2$ 的部分转换为 $\pm x^2\pm y^2,\pm x^2$ 或 0 的形式；然后再通过配方将尽可能多的线性部分消除

习题 1.4 对 1.3 中的仿射圆锥曲线和 1.6 中的射影圆锥曲线进行详细的比较

解答：(1). 非退化圆锥曲线, 对应椭圆、抛物线、双曲线;

(2). 空集, 对应 1.3 中 4、5、6 三种情况；

(3). 线对, 对应 7、8、9 三种情况；

(4). 单点, 对应 4；

(5). 双线, 对应 10；

另外, 视情况, 可认为整个射影平面对应 0=0；

将 1.3 的多项式所对应的矩阵化为只由 1 和-1 组成的对角形式的矩阵, 则 1.6 中从上到下的式子分别对应：$\begin{bmatrix}1&0&0\\0&1&0\\0&0&-1\end{bmatrix}\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\begin{bmatrix}1&0&0\\0&-1&0\\0&0&0\end{bmatrix}\begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix}\begin{bmatrix}1&0&0\\0&0&0\\0&0&0\end{bmatrix}$

习题 1.5　k 为特征值不为 2 的任意数域,V 是 k 上的三维向量空间,$Q:V\to k$ 是一个 V 上的非退化的二次型. 请证明如果 $0\neq e_1\in V$ 满足 $Q(e_1)=0$ 那么 V 有基底 e_1,e_2,e_3 使得 $Q(x_1e_1+x_2e_2+x_3e_3)=x_1x_3+ax_2^2$.

解答：设一对称双线性型满足：$\varphi(\alpha,\beta)=\alpha' A\beta$ (之后简写为 (α,β))

$Q(e_1)=0\Rightarrow\varphi(e_1,e_1)=0$

$\varphi(e_1,e_3)=1$

则 $Q(x_1e_1+x_2e_2+x_3e_3)=\varphi(x_1e_1+x_2e_2+x_3e_3,x_1e_1+x_2e_2+x_3e_3)=2x_1x_2(e_1,e_3)+2x_1x_3+x_2^2(e_2,e_2)+x_3^2(e_3,e_3)+2x_2x_3(e_2,e_3)$

下证 $\exists e_2\neq 0$ 使得 $(e_1,e_2)=0;(e_2,e_3)=0;(e_2,e_2)\neq 0$

首先

$$\begin{cases}(e_1,e_2)=0\\(e_3,e_2)=0\end{cases}\Rightarrow\begin{cases}(x_1y_1z_1)\,Ae_2=0\\(x_3y_3z_3)\,Ae_2=0\end{cases}\text{ 有解}$$

$\begin{bmatrix}(x_1y_1z_1)A\\(x_3y_3z_3)A\end{bmatrix}$ 秩 ≤ 2, 解空间维数 ≥ 1

$(e_1,e_2)=0,(e_3,e_2)=0$

若 $(e_2,e_2)=0,e_2=0$ 得出矛盾

故 $e_2\neq 0$

可得 $Q(x_1e_1+x_2e_2+x_3e_3)=2x_1x_3+x_2^2(e_2,e_2)+x_3^2(e_3,e_3)$

$e_3'=\lambda e_1+\mu e_3$(令 $\mu=1$)$\Rightarrow e_3'=-\frac{e_2e_3}{2}e_1+e_3$

最后再取 $e_1'=\frac{1}{\sqrt{2}}e_1,e_3''=\frac{1}{\sqrt{2}}e_3'$

得证

习题 1.6　设 k 是一个至少有 4 个元素的域,$C:(XZ=Y^2)\supset P_k^2$. 证明：如果 $Q(X,Y,Z)$ 是在 C 上为 0 的二次型, 则 $Q=\lambda(XZ-Y^2)$.

解答：带入特殊点即可, 可得 Q 所对应的矩阵为 $\begin{bmatrix}0&0&\lambda\\0&-2\lambda&0\\\lambda&0&0\end{bmatrix}$

习题 1.7 在 $\mathbb{R}^3$ 上, 考虑 $A:(Z=1)$ 和 $B:(X=1)$ 两个平面, 一条过原点的直线交平面 A 于 $(x,y,1)$, 交平面 B 于 $(1,\frac{y}{x},\frac{1}{x})$. 考虑由 $(x,y)\mapsto\left(y'=\frac{y}{x},z'=\frac{1}{x}\right)$ 定义的映射, 当原象为
(1) 直线族 $ax=y+b$ (其中 a 是定值而 b 是变量)
(2) 圆 $(x-1)^2+y^2=c$ 其中 c 是变量 (注意 c 的取值)
时, 考虑它的象. 并且指出当映射或逆映射没有定义时的情况.

解答: (1) 设参数 t, 则有 $ax=y+b$ 交 $A:(Z=1)$ 于 $(t,at-b,1)$, 参考题干给出的映射, 直线在 $B:(X=1)$ 上为 $(1,\frac{at-b}{t},\frac{1}{t})$. 则映射下的象为 $bz'=-y'+a$. 显然, 映射和逆映射总有定义.

(2) 设参数 θ, 取 $x=1+c\cos\theta,y=c\sin\theta$, 参考题干给出的映射, 有 $y'=\dfrac{c\sin\theta}{1+c\cos\theta},z'=\dfrac{1}{1+c\cos\theta}$. 则映射下的象为 $y'^2=(c^2-1)z'^2+2z'-1$, 当 $c<1$ 时是椭圆, 当 $c=1$ 时是抛物线, 当 $c>1$ 时是双曲线. 当映射没有定义时, 有 $x=0$, 即圆与 $A:(Z=1)$ 的交点为 $(0,y,1)$; 当逆映射没有定义时, 有 $x=\infty$, 即圆与 $A:(Z=1)$ 的交点为 $(\infty,y,1)$.

习题 1.8 $P_1,\cdots P_4$ 是 $\mathbb{P}^2$ 上任意三点不共线的四点. 证明: 存在一个仿射坐标系使得这四个点的坐标分别为 $(1,0,0),(0,1,0),(0,0,1)$ 和 $(1,1,1)$, 设 $P_5=(a,b,c)$ 是这四个点以外的第五个点, 找到所有经过这五个点的圆锥曲线并给出推论 1.10 和引理 1.11 的另外一个证明.

解答:设 $P_1,\cdots P_4$ 的坐标为 $(x_i,y_i,1),i=1,\cdots 4$. 考虑 $(x_i,y_i,1),i=1,\cdots 4$ 到 $(1,0,0),(0,1,0),(0,0,1),(1,1,1)$ 的仿射变换 $Ax+b=y$, 则有

$$\begin{pmatrix}a_{11}&a_{12}&a_{33}\\a_{21}&a_{22}&a_{23}\\a_{31}&a_{32}&a_{33}\end{pmatrix}\begin{pmatrix}x_1\\y_1\\1\end{pmatrix}+\begin{pmatrix}b_1\\b_2\\b_3\end{pmatrix}=\begin{pmatrix}1\\0\\0\end{pmatrix}$$
$$\begin{pmatrix}a_{11}&a_{12}&a_{33}\\a_{21}&a_{22}&a_{23}\\a_{31}&a_{32}&a_{33}\end{pmatrix}\begin{pmatrix}x_2\\y_2\\1\end{pmatrix}+\begin{pmatrix}b_1\\b_2\\b_3\end{pmatrix}=\begin{pmatrix}0\\1\\0\end{pmatrix}$$
$$\begin{pmatrix}a_{11}&a_{12}&a_{33}\\a_{21}&a_{22}&a_{23}\\a_{31}&a_{32}&a_{33}\end{pmatrix}\begin{pmatrix}x_3\\y_3\\1\end{pmatrix}+\begin{pmatrix}b_1\\b_2\\b_3\end{pmatrix}=\begin{pmatrix}0\\0\\1\end{pmatrix}$$
$$\begin{pmatrix}a_{11}&a_{12}&a_{33}\\a_{21}&a_{22}&a_{23}\\a_{31}&a_{32}&a_{33}\end{pmatrix}\begin{pmatrix}x_4\\y_4\\1\end{pmatrix}+\begin{pmatrix}b_1\\b_2\\b_3\end{pmatrix}=\begin{pmatrix}1\\1\\1\end{pmatrix}$$

由于 $P_1,\cdots P_4$ 任意三点不共线, 所以 $\begin{pmatrix}x_1&x_2&x_3&x_4\\y_1&y_2&y_3&y_4\\1&1&1&1\end{pmatrix}$ 是非奇异的, 因此可以解得 A 和 b, 则存在符合题意的仿射坐标系.

已知, 圆锥曲线在仿射变换下仍然为圆锥曲线, 因此我们只需要在仿射坐标系下进行证明. 显然, 存在圆锥曲线族经过 $(1,0,0),(0,1,0),(0,0,1)$ 和 $(1,1,1)$, 设为 A, 若存在一条圆锥曲线 C 经过这四个点及另外一点, 则有 $C\in A$, 将这样的 C 上的所有点的集合记为 P 并且有

$P \neq R^2, P \neq \emptyset$. 此时, 若 $P_5 \in P$, 则有且仅有一条圆锥曲线经过 $P_1, \cdots P_5$, 否则则没有这样的圆锥曲线.

习题 1.9 (1.12) 给出了两个圆锥曲线相交的所有可能性. 写下每种可能性对应的方程, 并找出对应的曲线族中的奇异曲线.(使用对称矩阵可能会比坐标系简单许多)

解答：因为圆锥曲线在仿射变换下不变, 因此不妨取其中一条圆锥曲线为 $x^2 + y^2 = 1$, 此时易得：

(1)$2x^2 + \dfrac{y^2}{2} = 1$

(2)$2x^2 + \dfrac{y^2}{2} = \dfrac{\sqrt{2}}{2}$

(3)$2x^2 + y^2 = 1$

(4)$(x + \dfrac{1}{2})^2 + y^2 = 1$

(5)$(x + \dfrac{1}{2})^2 + y^2 = \dfrac{1}{4}$

习题 1.10 (西尔维斯特行列式) 设 k 为代数闭域, U 为二次齐次多项式, Y 为三次齐次多项式, (按 (1.8) 节的定义):

$$q(U,V) = a_0U^2 + a_1UV + a_2V^2$$
$$c(U,V) = b_0U^3 + b_1U^2V + b_2UV^2 + b_3V^3$$

证明 q 和 c 有一个公共的零点 $(\eta : \tau) \in \mathbb{P}^1$ 当且仅当

$$\det \begin{vmatrix} a_0 & a_1 & a_2 & 0 & 0 \\ 0 & a_0 & a_1 & a_2 & 0 \\ 0 & 0 & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & b_3 & 0 \\ 0 & b_0 & b_1 & b_2 & b_3 \end{vmatrix} = 0$$

证明：记

$$Res(q,c) = det \begin{vmatrix} a_0 & a_1 & a_2 & 0 & 0 \\ 0 & a_0 & a_1 & a_2 & 0 \\ 0 & 0 & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & b_3 & 0 \\ 0 & b_0 & b_1 & b_2 & b_3 \end{vmatrix}$$

必要性：证法一：若 $(1,0)$ 是公共解, 则 $a_0 = b_0 = 0$, 所以 $Res(q,c) = 0$.

若 $(1,0)$ 不是公共解, 则

$$\begin{cases} q(x) = a_0x2 + a_1x + a_2 \\ c(x) = b_0x^3 + b_1x^2 + b_2x + b_3 \end{cases}$$

有公共解 $\frac{\eta}{\tau} = x_0$.

所以 $q(x), c(x)$ 可分解成

$$\begin{cases} q(x) = q_1(x)(x - x_0) \\ c(x) = c_1(x)(x - x_0) \end{cases}$$

其中 $q_1(x)$ 为一次多项式,$c_1(x)$ 为二次多项式, 设为 $q_1(x) = u_0x + u_1, c_1(x) = v_0x^2 + v_1x + v_2$. 所以

$$c_1(x)q(x) = q_1(x)c(x) \qquad (*)$$

比较 (*) 式多项式两边的系数可得

$$\begin{cases} a_0v_0 = b_0u_0 \\ a_1v_0 + a_0v_1 = b_0u_1 + b_1u_0 \\ a_2v_0 + a_1v_1 + a_0v_2 = b_1u_1 + b_2u_0 \\ a_2v_1 + a_1v_2 = b_3u_0 + b_2u_1 \\ a_2v_2 = b_3u_1 \end{cases} \qquad (**)$$

由于 $q(x) \neq 0, c(x) \neq 0$, 所以 $q_1(x) \neq 0, c_1(x) \neq 0$, 即 $(v_0, v_1, v_2, -u_0, -u_1) \neq 0$.

(**) 对应的齐次方程有非零解 $(v_0, v_1, v_2, -u_0, -u_1)$, 所以

$$det \begin{vmatrix} a_0 & 0 & 0 & b_0 & 0 \\ a_1 & a_0 & 0 & b_1 & b_0 \\ a_2 & a_1 & a_0 & b_2 & b_1 \\ 0 & a_2 & a_1 & b_3 & b_2 \\ 0 & 0 & a_2 & 0 & b_3 \end{vmatrix} = 0$$

进而 $Res(q, c) = 0$.

证法二：如果 q, c 有公共解, 则 U^2q, UVq, V^2q, Uc, Vc 有公共零解 $(\eta : \tau) \in P^1$, 其中

$$\begin{cases} U^2q = a_0U^4 + a_1U^3V + a_2U^2V^2 \\ UVq = a_0U^3V + a_1U^2V^2 + a_2UV^3 \\ V^2q = a_0U^2V^2 + a_1UV^3 + a_2V^4 \\ Uc = b_0U^4 + b_1U^3V + b_2U2V^2 + b_3UV^3 \\ Vc = b_0U^3V + b_1U^2V^2 + b_2UV^3 + b_3V^4 \end{cases}$$

所以 $S((\eta : \tau)) = k_1U^4 + k_2U^3V + k_3U^2V^2 + k_4UV^3 + k_5V^4$ 同构于 R^4,

所以 5 个向量 $(a_0, a_1, a_2, 0, 0), (0, a_0, a_1, a_2, 0), (0, 0, a_0, a_1, a_2), (b_0, b_1, b_2, b_3, 0), (0, b_0, b_1, b_2, b_3)$ 是线性相关的, 即得 $Res(q, c) = 0$.

充分性：$Res(q, c) = 0$, 则齐次方程

$$\begin{cases} a_0x_1 + b_0x_4 = 0 \\ a_1x_1 + a_0x_2 + b_1x_4 + b_0x_5 = 0 \\ a_2x_1 + a_1x_2 + a_0x_3 + b_2x_4 + b_1x_5 = 0 \\ a_2x_2 + a_1x_3 + b_3x_4 + b_2x_5 = 0 \\ a_2x_3 + b_3x_5 = 0 \end{cases}$$

有非零解, 设为 $(v_0, v_1, v_2, -u_0, -u_1) \neq 0$, 代入上面的方程即可得到 (**) 式.

由

$$q(x) = a_0x^2 + a_1x + a_2$$
$$c(x) = b_0x^3 + b_1x^2 + b_2x + b_3$$
$$q_1(x) = u_0x + u_1$$
$$c_1(x) = v_0x^2 + v_1x + v_2$$

可以得到 (*) 式, 且 $degq_1(x) < 2, degc_1(x) < 3$

当 a_0, b_0 不全为 0 时, 不妨假设 $a_0 \neq 0$, 则 $degq(x) = 2$, 由 (*), $q(x)|q_1(x)c(x)$, 反设 $q(x), c(x)$ 无公共零点, 则 $(q(x), c(x)) = 1$, 所以 $q(x)|q_1(x)$, 则 $degq(x)$ 小于等于 $degq_1(x) < 2$, 矛盾, 所以 $q(x), c(x)$ 有公共零点, 设为 α , 则 $(\alpha, 1)$ 是 $q(U, V), c((U, V)$ 的公共零解.

当 a_0, b_0 全为 0 时, 易得 $q(U, V), c((U, V)$ 有公共零解 $(1, 0)$.

习题 1.11　把习题 1.10 的结果推广到 U, Y 为任意 n 和 m 次的两种形式中.

设 k 为代数闭域,f,g 分别是关于 U,V 的 n 次,m 次齐次形式,

$$f(U, V) = a_0U^n + a_1U^{n-1}V + \cdots + a_{n-1}UV^{n-1} + a_nV^n$$
$$g(U, V) = b_0U^m + b_1U^{m-1}V + \cdots + b_{m-1}UV^{m-1} + a_mV^m$$

f 和 g 有一个公共的零点 $(\eta : \tau) \in P^1$ 当且仅当

$$det \begin{vmatrix} a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 & 0 & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\cdots & \\ 0 & 0 & \cdots & 0 & \cdots & a_0 & a_1 & \cdots & a_n \\ b_0 & b_1 & \cdots & \cdots & b_m & 0 & \cdots & 0 & 0 \\ 0 & b_0 & b_1 & \cdots & \cdots & b_m & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\cdots & \\ 0 & \cdots & \cdots & 0 & b_0 & b_1 & \cdots & \cdots & b_m \end{vmatrix} = 0$$

Chapter 2

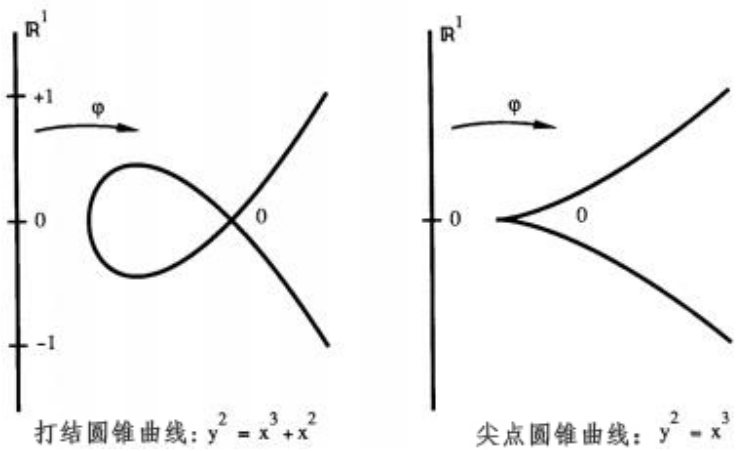
三次曲线和群定律

2.1 三次曲线参数化的例子

正如二次曲线那样, 一些平面三次曲线可以参数化:

结点三次曲线 $C:(y^2=x^3+x^2)\subset R^2$ 是映射 $\phi:R^1\to R^2, t\longmapsto(t^2-1,t^3-t)$ 的象.

尖点三次曲线 $C:(y^2=x^3)\subset R^2$ 是映射 $\phi:R^1\to R^2, t\longmapsto(t^2,t^3)$ 的象.



想想图像曲线和映射的奇点, 这些例子会贯穿整个课程, 所以花点时间来处理这些方程; 见练习 *2.1-2.*

2.2 曲线 $(y^2=x(x-1)(x-\lambda))$ 没有有理参数化

参数化曲线很好; 例如, 如果您对丢番图问题感兴趣, 您可以期望一个表达式给出所有有理值点, 如 (1.1) 所示.(1.1) 的参数化形式为 $x=f(t), y=g(t)$, 其中 f 和 g 是有理函数, 即两个多项式的商.

定理 k 是一个特征不为 2 的域, $\lambda\in k$ 且 $\lambda\neq 0,1, f,g\in k(t)$ 是有理函数, 满足 $(f^2=g(g-1)(g-\lambda)$, 则 $f,g\in k$.

这相当于说不存在任何由有理函数给出的非常数映射 $R^1\to C:(y^2=x(x-1)(x-\lambda))$.

定理的证明是在 $k(t)$ 中利用 $k(t)$ 是唯一分解环 $k[t]$ 的分式域的事实.

证明 $k[t]$ 是唯一分解环, 设 $f = r/s, r, s \in k[t]$ 且互素, $g = p/q, p, q \in k[t]$ 且互素, 代入 $(f^2 = g(g-1)(g-\lambda)$ 得 $\frac{r^2}{s^2} = \frac{p}{q}(\frac{p}{q}-1)(\frac{p}{q}-\lambda)$, 除去公分母后得, $r^2q^3 = s^2p(p-q)(p-\lambda q)$, 因为 r 和 s 是互素的, 右边的因子 s^2 一定整除 q^3. 同理, 因为 p 和 q 是互素的, 左边的因子 q^3 一定整除 s^2. 所以,$s^2|q^3$ 且 $q^3|s^2$, 所以 $s^2 = aq^3$, 其中 $a \in k(a$ 是 $k[t]$ 中的单位, 所以 $a \in k)$.

可得 $aq = (\frac{s}{q})^2$ 是 $k[t]$ 中的平方形式. 并且 $r^2 = ap(p-q)(p-\lambda q)$, 所以考虑分解到素元的因式分解, 存在非零常数 $b, c, d \in k$ 使 $bp, c(p-q), d(p-\lambda q)$ 是 $k[t]$ 中的平方形式. 下面如果能证明 p, q 是常数, 那么 r, s 也是, 定理得证. 为了证明 p, q 是常数, 设 K 是 k 的代数闭包; 那么 $p, q \in K[t]$ 满足以下引理的条件.

2.3 引理

K 是一个代数闭域, $p, q \in K[t]$ 互素, 假设 4 个不同的线性组合 $(\lambda p + \mu q$, 4 个不同的比例 $(\lambda : \mu) \in P^1_k)$ 为 $K[t]$ 中的平方形式. 那么 $p, q \in K$.

证明 (费马无穷递降法) 将 p, q 替换成 $p' = ap + bq, q' = cp + dq$, 其中 $a, b, c, d \in K$ 并且 $ad - bc \neq 0$, 不会影响定理的假设和结论, 因此我可以假设 4 个给定的平方形式是 $p, p-q, p-\lambda q, q$. 那么 $p = u^2, q = v^2$, 并且 $u, v \in K[t]$ 互素, 则 $max\{degu, degv\}$ 小于 $max\{degp, degq\}$. 假设 $max\{degp, degq\}$ 大于 0, 并且是满足引理条件的 p, q 中次数最小的, 那么 $p-q = u^2-v^2 = (u-v)(u+v)$ $p-\lambda q = u^2-\lambda v^2 = (u-\mu v)(u+\mu v)$(其中 $\mu = sqrt\lambda$) 是 $K[t]$ 中的平方形式. 所以根据 u, v 互素的形式, 可得每个 $u-v, u+v, u+\mu v, u-\mu v$ 都是平方形式. 这与 $max\{degp, degq\}$ 的极小性矛盾. 所以 $max\{degp, degq\} = 0, p, q \in K$.

2.4 线性系统

记 S_d=(X, Y, Z) 的 d 次型 (这个形式是齐次多项式), 任意元素 $F \in S_d$ 可以唯一地写成

$$F = \sum a_{ijk} X^i Y^j Z^k, a_{ijk} \in k$$

i+j+k=d; 这意味着 S_d 是一个 k 上的向量空间, 它有基底

$$\begin{array}{c} Z^d \\ Z^{d-1}X \quad Z^{d-1}Y \\ .. \quad .. \\ X^{d-1}Z \quad X^{d-2}YZ.. \quad Y^{d-1}Z \\ X^d \quad X^{d-1}Y \quad X^{d-2}Y^2 \quad .. \quad Y^d \end{array}$$

特别的,$dimS^d$= $\begin{pmatrix} d+2 \\ 2 \end{pmatrix}$. 对于 $P_1, ...P_n \in P^2$, 令

$$S_d(P_1, ..P_n) = \{F_E S_d | F(P_i) = 0, i = 1, 2, ...n\} \subset S_d$$

对于每个条件 $F(P_i) = 0$,(或者更精确一点,$F(X_i, Y_i, Z_i = 0, P_i = (X_i : Y_i : Z_i))$ 是 F 上的线性条件, 使得 $S_d(P_1, ..P_n)$ 是一个维数 $\geq \begin{pmatrix} d+2 \\ 2 \end{pmatrix} - n$ 的向量空间.

2.5 引理

设 k 是一个无限域,$F \in S_d$.

(i) 记 $L \subset \mathbb{P}_k^2$ 为一条直线, 如果在 L 上 $F \equiv 0$, 那么 F 由 L 的方程在 $k[X,Y,Z]$ 上是可分的. 这是说,$F = H \cdot F'$ 成立, 当 H 是 L 的方程且 $F' \in S_{d-1}$

(ii) 记 $C \subset \mathbb{P}_k^2$ 是一条非空非退化的圆锥曲线, 如果在 C 上 $F \equiv 0$,, 那么 F 由 C 的方程在 $k[X,Y,Z]$ 上是可分的. 这是说,$F = Q \cdot F'$ 成立, 当 Q 是 C 的方程且 $F' \in S_{d-1}$ 证明.(i) 通过坐标变换, 我们可以假定 $L = X$, 那么对于任意的 $F \in S_d$, 存在唯一一个表达式 $F = X \cdot F'_{d-1} + G(Y,Z)$: 只需把所有含 X 的单项式集中到第一个被加数里, 剩下的就必然只有含 Y,Z 的多项式. 现在有在 L 上 $F \equiv 0 \Leftrightarrow$ 在 L 上 $G \equiv 0 \Leftrightarrow G(Y,Z) = 0$. 最后一步是由于 (1.7): 如果 $G(Y,Z) \neq 0$, 那么它在 $\mathbb{P}_k^1$ 上至多有 d 个零点, 然而如果 k 是无限域, 那么对于 $\mathbb{P}_k^1$ 也一样.

(ii) 通过坐标变换,$Q = XZ - Y^2$. 现在证明对任意 $F \in S_d$, 都存在唯一一个表达式 $F = Q \cdot F'_{d-2} + A(X,Z) + YB(X,Z)$: 如果用 $(XZ - Q)$ 来代替 Y^2, 那么剩下的部分 Y 的次数就一定不大于 1, 故是 $A(X,Z) + YB(X,Z)$ 的形式. 正如在 (1.8) 中,C 是一个由 $X = U^2, Y = UV, Z = V^2$ 参数化的圆锥曲线, 使得

$$\begin{aligned} C\text{上}F \equiv 0 &\Leftrightarrow C\text{上}A(U^2,V^2) + UVB(U^2,V^2) \equiv 0 \\ &\Leftrightarrow A(U^2,V^2) + UVB(U^2,V^2) = 0 \in k[U,V] \\ &\Leftrightarrow A(X,Z) = B(X,Z) = 0 \end{aligned}$$

分开考虑 $A(U^2,V^2) + UVB(U^2,V^2)$ 的奇次项和偶次项最后一个等式可以得到最后一个等式. 证毕.

练习 *2.2* 给出了明确的零点定理的相似例子.

推论 令 $L : (H = 0) \subset \mathbb{P}_k^2$ 为一条直线 (另外的 $C : (Q = 0) \subset \mathbb{P}_k^2$ 是一条非退化圆锥曲线); 假设给定点 $P_1, P_2 ... P_n \in P_k^2$, 考虑 $S_d(P_1, P_2 ... P_n), d$ 已给定. 那么

(i) 如果 $P_1, P_2 ... P_a \in L, P_{a+1}, P_{a+2} ... P_n \notin L$, 且 $a > d$, 那么

$S_d(P_1, P_2 ... P_n) = H \cdot S_{d-1}(P_{a+1}, P_2 ... P_n)$

(ii) 如果 $P_1, P_2 ... P_a \in C, P_{a+1}, P_{a+2} ... P_n \notin C$, 且 $a > 2d$, 那么

$S_d(P_1, P_2 ... P_n) = Q \cdot S_{d-2}(P_{a+1}, P_2 ... P_n)$

证明: 如果 F 是一个 d 次齐次多项式, 曲线 $D : (F = 0)$ 与 L 相交于 $P_1 ... P_a$ 当 $a > d$, 那么由 (1.8), 就一定有 $L \subset D$, 使得由引理可知 $F = H \cdot F$; 由于 $P_{a+1}, ..., P_n \notin L$, $F \in S_{d-1}(P_{a+1} ... P_n)$. 同理可得 (ii) 的结论. 证毕.

2.6 命题

令 k 是一个无限域,$P_1 ... P_8 \in \mathbb{P}_k^2$ 是两两不同的点, 如果这 8 点中没有任意两点共线, 而且没有任意 7 点在同一个非退化圆锥曲线上, 那么

$$dim S_3(P_1 ... P_8) = 2$$

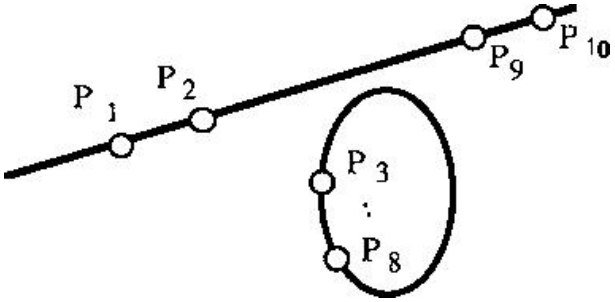
证明 (2.6) 的证明分几种情况.

大多数情况 没有任意 3 点共线, 没有任意 6 点共圆锥曲线. 这是一般的位置情况.

假设 $dimS_3(P_1...P_8) \geq 3$, 然后令 P_9, P_{10} 是直线 $L = P_1P_2$. 那么

$$dimS_3(P_1...P_{10}) \geq dimS_3(P_1...P_8) - 2 \geq 1$$

所以有 $0 \neq F \in S_3(P_1...P_{10})$. 由定理 2.5,$F = H \cdot Q, Q \in S_2(P_3...P_8)$. 现在可以得出矛盾: 如果 Q 是非退化的那么 $P_3...P_8$ 是共圆锥曲线的, 然而如果 Q 是线对或二重线, 那么它们中至少 3 点共线.



第一退化情况 设 $P_1P_2P_3 \in L$ 是共线的, 令 $L : (H = 0)$. 令 P_9 是 L 上的第四个点, 那么由定理 2.5,

$$S_3(P_1...P_9) = H \cdot S_2(P_4...P_8)$$

同样, 由于 $P_4...P_8$ 是共线的, 由 1.9,$dimS_2(P_4...P_8) = 1$, 并且 $dimS_3(P_1...P_9) = 1$, 这意味着 $dimS_3(P_1...P_8) \leq 2$

第二退化情况 设 $P_1...P_6 \in C$ 是共圆锥曲线的,$C : (Q = 0)$ 是一个非退化圆锥曲线. 那么选择区别于 $P_1...P_6$ 的 $P_9 \in C$, 由定理 2.5,

$$S_3(P_1...P_9) = Q \cdot S_1(P_{7,8})$$

线 $L = P_7P_8$ 是唯一的, 所以 $S_3(P_1...P_9)$ 是由 QL 限制的一维空间, 因此 $dimS_3(P_1...P_8) \leq 2$. 证毕.

2.7 定理

C_1C_2 是两条圆锥曲线, 它们的交点是 9 个两两不同的点,$C_1 \cap C_2 = P_1...P_9$. 那么圆锥曲线 D 如果通过 $P_1...P_8$, 也必然穿过 P_9.

证明 如果 $P_1...P_9$ 中的 4 个点在一条线 L 上, 那么 C_1C_2 的每一条都会与 L 相交于 4 个点以上, 因此就包含直线 L 这与 $C_1 \cap C_2$ 的假设矛盾. 同样的, 不能有 7 个点共圆锥曲线. 因此满足了 2.6 的假设, 所以

$$dimS_3\left(P_1 \ldots P_8\right) = 2$$

这意味着 C_1, C_2 的等式 F_1, F_2 构成了 $S_3(P_1...P_8)$ 的基. 因此 $D : (G = 0)$, 其中 G=λF_1+μF_2. 现在 F_1, F_2 在 P_9 上退化, 因此 G 也一样. 证毕.

2.8 平面三次曲线的群论

假设 $k \subset C$ 是 C 的子域,$F \in k[X,Y,Z]$ 是一个定义了一个非空平面曲线 C 的三次型,C : $(F=0) \subset \mathbb{P}^2_k$. 假定 F 满足以下两条性质：

(a) F 是不可约的 (这样 C 就不会包含一条直线或圆锥曲线)；

(b) 对于任意一点 $P \in C$, 都存在唯一一条 $L \subset \mathbb{P}^2_k$ 使得 P 是 $F|_L$ 的重根.

几何上, 条件 (b) 要求 C 是非奇异的,L 指的是切线 $L = T_P C$(见练习 *2.3*).

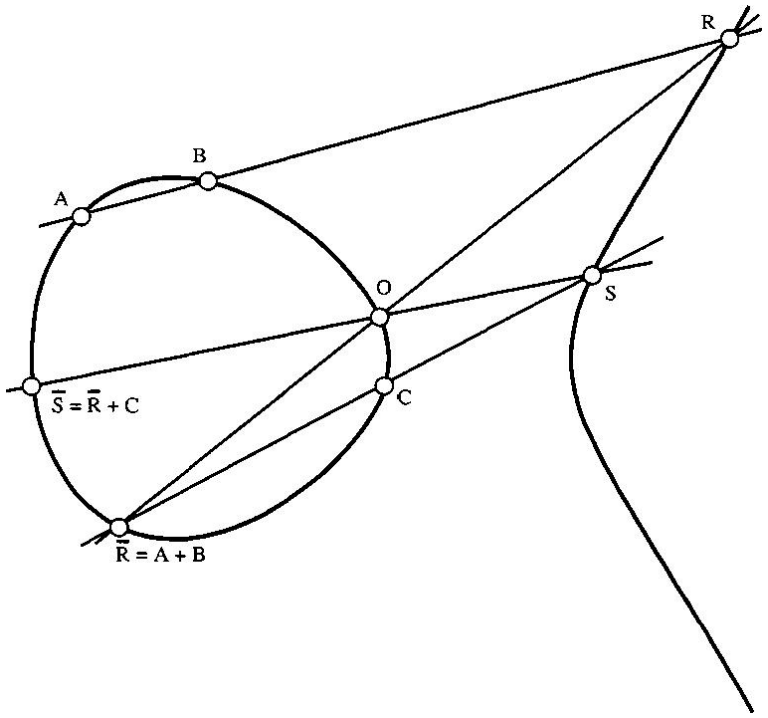
固定任意一点 $O \in C$, 进行下列构造：

构造 (i) 对 $A \in C$, 令 $\overline{A}$ 为 C 与 OA 的第三个交点；

(ii) 对于 $A, B \in$C, 记 R 为 AB 与 C 的第三个交点, 定义 $A + B = \overline{R}$.

定理 结合性是这里的关键.

(I) 需证明加法和逆运算是良定义的. 如果 P, Q 是 C 上任意两点, 那么 $P \neq Q$, 这样 $L = PQ \subset P^2_k$ 是唯一确定的, 不然由假设 (b) 知 $P = Q$, 那么有唯一一条直线 $L \subset \mathbb{P}^2_k$ 使得 P 是 $F|_L$ 的重根；在另一种情况下,$F|_L$ 是有两个变量的三次型, 有两个 k 上的零点. 因此它分为 3 个线性因式的乘积, 故无一例外的, 第三个交点 R 是良定义的而且在 k 内有坐标. 注意 $P = Q, P = R, Q = R, P = Q = R$ 都是可以的. 这在代数上与 $F|_L$ 有多个零点一致, 在几何上与切线和回折点一致.



(II) 验证零元 O 点是符合零元条件的：$OA\overline{A}$ 是共线的,$O + A$ 由 $L = OA$ 得到第三个交点 $\overline{A}$, 则同一条线 $L = O\overline{A}$ 得到 A, 得证.

(III)$A + B = B + A$ 显然. (IV) 先由 (i) 定义点 $\overline{O}$：令 L 为使得 O 是 $F|_L$ 重根的直线, 定义 $\overline{O}$ 是 L 与 C 的第三个交点. 那么显然对任意 $A \in C$,$\overline{O}A$ 的第三个交点都是 A 的逆.

2.9

现在, 我们给出一个“足够普遍”的情况下的结合律的证明：假设 A, B, C 是三次曲线 C 上的三点, 而 $(A+B)+C=\overline{S}$ 的构造用到了四条直线 (如上一节图):

$$L_1 : ABR, L_2 : RO\overline{R}, L_3 : C\overline{R}S, L_4 : SO\overline{S}$$

$(B+C)+A=\overline{T}$ 的构造则用到了另外四条直线:

$$M_1 : BCQ, M_2 : QO\overline{Q}, M_3 : A\overline{Q}T, M_4 : TO\overline{T}$$

我们需要证明 $\overline{S}=\overline{T}$, 显然, 只需要证明 $S=T$ 即可. 考虑三次曲线：

$$D_1 = L_1 + M_2 + L_3 \text{ 和} D_2 = M_1 + L_2 + M_3$$

由构造可知,

$$C \cap D_1 = \{A, B, C, O, R, \overline{R}, Q, \overline{Q}, S\}$$

$$C \cap D_2 = \{A, B, C, O, R, \overline{R}, Q, \overline{Q}, T\}$$

已知,$A, B, C, O, R, \overline{R}, Q, \overline{Q}, S$ 这九个点都是独立的, 三次曲线 C 和 D_1 满足推论 2.7 的条件, 因此,D_2 一定经过 S, 而这当且仅当 $S=T$ 时成立.

完成这个证明有很多方法, 其中最彻底的证明给出了考虑多交点的两条曲线的交点的真实处理方法, 而对应推论 2.7 的证明是 Max Noether 的引理.

2.10

在这里, 我们给出一个利用连续性的证明, 这个证明将用到 $k \in \mathbb{C}$ 这个事实. 对曲线 C 考虑对应的复曲线 $C_{\mathbb{C}} \subset \mathbb{P}^2_{\mathbb{C}}$, 即当 $(X:Y:Z)$ 在复数域上时仍然有 $F(X,Y,Z)=0$. 而如果结合律在复曲线 $C_{\mathbb{C}}$ 上成立, 那么显然在曲线 C 上也处处成立. 因此, 我们不妨假设 $k=\mathbb{C}$.

引理 (i)$A+B$ 是对于 A 和 B 的连续函数.

(ii) 对于所有 $A, B, C \in C$ 存在任意近的三点 $A', B', C' \in C$ 使得构造出来的九点 $A', B', C', O, R, \overline{R}, Q, \overline{Q}, S$ 都是独立的.

加法 $\varphi : C \times C \to C$ 是一个由 $(A, B) \mapsto A+B$ 定义的映射. 由 (i),φ 是连续的, 因此有两个映射 $f=\varphi\circ(\varphi\times id_C)$ 和 $g=\varphi\circ(id_C\times\varphi) : C\times C\times C \to C$ 分别由 $(A,B,C)\mapsto(A+B)+C$ 和 $A+(B+C)$ 定义. 并且, 由 (ii), 能使这九个点的构造是独立的子集 $U \subset C\times C\times C$ 由 (A,B,C) 组成, 并且是稠密的；由上面的证明,f 和 g 在 U 上总相等, 则由连续性, 它们处处相等.

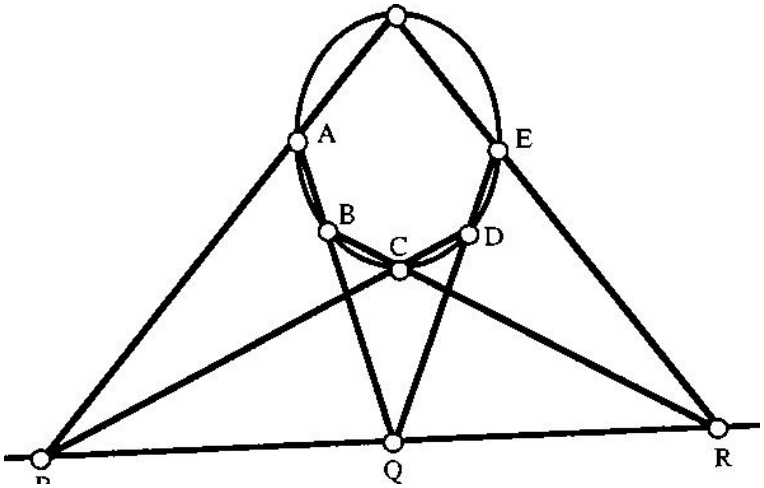
注 连续性的证明是建立在 $\mathbb{C}$ 的拓扑上的, 因此这个证明不是纯代数的. 事实上加法映射 φ 是 $\varphi : C\times C \to C$ 的一个态射, 并且会在 (4.14) 证明, 而剩下的部分可以重构成纯代数的形式：$C\times C\times C$ 的能使这九个点的构造是独立的子集是 Zariski 拓扑上的紧开集, 而在紧开集上相等的两个态射处处相等.

2.11 帕斯卡定理

(神秘六边形) 图中是一个平面 $\mathbb{P}^2_k$ 中六边形 $ABCDEF$, 它的对边延伸直至相交到点 P, Q, R. 假设这九个点和六条边都是不同的; 则

$$ABCDEF\text{共圆锥曲线} \iff PQR\text{共线}$$

这个著名的定理是 2.7 的一个相当相似的应用, 给出它只是为了好玩；当然其它证明也是可以的, 参见任何版本的几何书, 如 [Berger,16.2.10 和 16.8.3-5].



证明 在图中, 考虑两组直线

$$L_1 : PAF, L_2 : QDE, L_3 : RBC$$

和

$$M_1 : PCD, M_2 : QAB, M_3 : REF$$

令 $C_1 = L_1 + L_2 + L_3, C_2 = M_1 + M_2 + M_3$, 应用 2.7, 显然 C_1 和 C_2 是两条三次曲线且满足

$$C_1 \cap C_2 = \{A, B, C, D, E, F, P, Q, R\}$$

假如 PQR 共线, $L = PQR$; 令 Γ 为过 $ABCDE$ 的圆锥曲线 (其存在唯一性由推论 1.11 给出). 然后, 通过构造,$L + \Gamma$ 是一条通过 8 个点 A, B, C, D, E, P, Q, R 的三次曲线, 则通过 (2.7), 它一定通过点 F, 即 $F \subset L \cup \Gamma$; 根据假设 $F \notin L$, 所以 $F \in \Gamma$, 故六点共圆锥曲线.

反过来, 假设 $ABCDEF$ 在一个圆锥曲线 Γ 上, 令 $L = PQ$, 则 $L + \Gamma$ 是一个通过 A, B, C, D, E, F, P, Q 的三次圆锥曲线, 由 2.7 知, 它一定通过 R. R 不可能在圆锥曲线 Γ 上 (否则 Γ 是一对直线或图中 6 条线中的一些会重合), 所以 $R \in L$, 即 PQR 共线.

2.12 拐点, 标准形式

$\mathbb{P}^2_R$ 或 $\mathbb{P}^2_C$ 中有能被写成标准形式

$$C : Y^2Z = X^3 + aXZ^2 + bZ^3$$

或仿射形式

$$C : y^2 = x^3 + ax + b$$

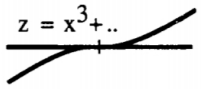
的曲线

现在考虑上述曲线 C; 它与无穷远直线 $L : (Z = 0)$ 在何处相交？那很容易, 只要把 $Z = 0$ 代入 $F = -Y^2Z + X^3 + aXZ^2 + bZ^3$ 得到 $F|_L = X^3$; 这意味着 $F|_L = X^3$ 在 $P(0, 1, 0)$ 处有一个三重零点.

为了看看这在几何上代表什么, 令 $Y = 1$, 得到 $(0, 1, 0)$ 附近关于仿射坐标 (x, z) 的方程：

$$C : z = x^3 + axz^2 + bz^3$$

这个曲线高度近似于 $z = x^3$:



这说明 C 在 $(0, 1, 0)$ 处有一个拐点.

更一般地,C 上有一个拐点 P 的定义是存在一条直线 $L \subset \mathbb{P}^2_k$, 使 $F|_L$ 在 P 点有一个重数大于等于 3 的零点 (见习题 2.9；事实上需要 $L = T_PC(2.8, b)$ 且重数 =3(1.9)), 不难用定义方程的导数和二阶导数来说明这一点, 如果定义方程是 $y = f(x)$, 那么 P 为拐点的条件是,$\frac{d^2f}{dx^2(P)} = 0$, 这在图中对应一个从凹向下到凹向上变化的曲线. 根据 Hessian 得知平面曲线是否有拐点有一个标准, 见 [Fulton,p.116] 或练习 *7.3*,(iii).

反过来, 如果一条曲线 C 有拐点, 那么它的表达式一定能写成标准形式 $C : Y^2Z = X^3 + aXZ^2 + bZ^3$.

2.13 简化的群

在标准形式 P^2_R 或 P^2_C 中有能被写成标准形式

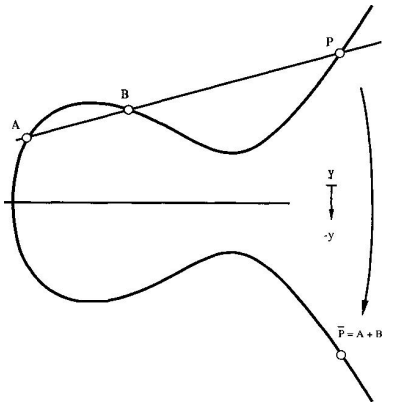
$$C : Y^2Z = X^3 + aXZ^2 + bZ^3$$

的曲线上定义群很方便：将点 $O(0, 1, 0)$ 作为零元. 在这些条件下, 群的建立会很好, 有以下几点原因：

(a)$C = O \cup C_0 : (y^2 = x^3 + ax + b)$, 所以可将曲线 C 看作一条仿射曲线和无穷远一点 O, 即群的零元.

(b) 过 O 的直线是 (2.8)(i) 群的构造的主要部分, 由 $X = \lambda Z$ 给出, 仿射坐标系中为 $x = \lambda$; 这样的直线与 C 的交点或者是 $(\lambda, \pm\sqrt{\lambda^3 + a\lambda + b})$, 或者是无穷远点 O. 因此如果点 P 的坐标为 (x, y), 则 (2.8,i) 中构造的 $\bar{P}$ 为 $(x, -y)$, 所以映射 $P \mapsto \bar{P}$ 由 $(x, y) \mapsto (x, -y)$ 给出.

(c) 由 (2.8,IV), 群的逆由 $\bar{O}$ 给出,$\bar{O}$ 是以 O 为 2 重零点的直线 L 与 C 的第三个交点；在我们现在的情况下, 这条直线是无穷远直线 $L : (Z = 0)$ 且 $L \cap C = 3O$, 所以 $\bar{O} = O$, 群的逆简化为 $-P = \bar{P}$.



定理 C 是由标准形式 $C: Y^2Z = X^3 + aXZ^2 + bZ^3$ 给出的一条三次曲线, 那么在 C 上有唯一的群使得 $O = (0, 1, 0)$ 是零元, 元素的逆由由 $(x, y) \mapsto (x, -y)$ 给出, 且对任意的 $P, Q, R \in C$,

$$P + Q + R = O \Longleftrightarrow P, Q, R\text{共线}$$

证明 左 $\Rightarrow$ 右 $P + Q = -R = \bar{R}$, 所以 PQ 与 C 的第三的交点为 R, 即 P, Q, R 共线.

右 $\Leftarrow$ 左 $P + Q = \bar{R} = -R$, 所以 $P + Q + R = O$.

练习 2

习题 2.1 在 $C: (y^2 = x^3 + 4x)$ 上建立如 (2.13) 给出的简化群律. 证明: 曲线 C 在 $P = (2, 4)$ 处的切线经过 $(0, 0)$, 并且 P 在群中是四阶元.

证明:

联立方程 $\begin{cases} y^2 = x^3 + 4x \\ y = 2x \end{cases}$ 得到方程在 $(0, 0)$ 处有一个根, 在 $(2, 4)$ 处有一个二重根.

根据习题 2.3 的结论, 显然经过 (0,0) 和 (2,4) 的直线是曲线 C 在 (2,4) 的切线.

设 (0,0) 为点 A, 根据 (2.13) 给出的简化群律,$P+P = A$, 同时 $A+A = O$, 则此时有 $4P = O$ 即 P 是四阶元.

习题 2.2 曲线 $C: (y^2 = x^3 + ax + b) \subset \mathbb{R}^2$ 是非奇异的, 找出建立在曲线上的群中所有的二阶元并解释所有二阶元形成的群 (这可以分成两种情况), 然后几何性地解释如何找出所有的四阶元.

解:

对于方程 $x^3 + ax + b = 0$, 显然它的解有两种情况:

1. 有一个实根和两个虚根, 设实根为 $x = a$

在这种情况下, 点 $(a, 0)$ 是唯一的二阶元, 此时所有二阶元组成的群是二阶循环群.

2. 有三个实根, 设实根分别为 $x = a$,$x = b$,$x = c$

在这种情况下, 点 $(a, 0)$,$(b, 0)$,$(c, 0)$ 都是二阶元, 并且所有二阶元组成的群是克莱因四元群.

根据习题 2.4 的结论, 所有四阶元处的切线都经过二阶元, 则过二阶元作曲线的切线可找出所有的四阶元.

习题 2.3 x, z 是 k^2 上的一组基底, 对 $f \in k[x, z]$ 有

$$f = a + bx + cz + dx^2 + exz + fz^2 + \dots$$

当 f 递进地满足下列条件时, 写出参数 $a, b, c \dots$ 的取值

(i) $P = (0, 0) \in C : (f = 0)$;

(ii) C 在 P 点处的切线是 $(z = 0)$;

(iii) P 是 C 上的拐点并且 $(z = 0)$ 是切线.

解:

(i) 将 $P(0, 0)$ 点代入方程, 得 $a = 0$.

(ii) 将隐函数 $a + bx + cz + dx^2 + exz + fz^2 + \dots = 0$ 对 x 求导, 得 $b + cz' + 2dx + ez + exz' + 2fzz' + \dots = 0$

将 $x = 0, z' = 0$ 代入, 得 $b = 0$

(iii) 联立方程 $\begin{cases} f = 0 \\ z = 0 \end{cases}$ 由 (2.12) 知方程在 (0,0) 处有三重及以上重数的根, 即 $c = 0, f = 0$

Chapter 3

仿射簇和希尔伯特零点定理

前半部分大多是纯交换代数. 在这一章中, 环意味着有单位元的交换环.

3.1 命题与定义

下面的条件对于环 A 来说等价.

(i) 每个理想 $I \subset A$ 是有限生成的. 即, 任意理想 $I \subset A$, 存在 $f_1, ..., f_k \in A$, 使得 $I = (f_1, ..., f_k)$.

(ii) 每一条 A 的理想构成的升链

$$I_1 \subset ... \subset I_m \subset ...$$

会终止, 即有 $I_N = I_{N+1} = ...$(升链条件,a.c.c).

(iii)A 的非空理想有极大元.

满足以上三个条件,A 称为诺特环.

证明 $(i) \Rightarrow (ii)$ 假定 $I_1 \subset ... \subset I_m \subset ...$, 设 $I = \bigcup I_m$ 显然 I 仍为理想. 如果 $I = (f_1, ..., f)$, 那么任意 f_i 都是 $I_(m(i))$ 的元素, 所以取 $m = max(m(i))$ 令 $I = I_m$, 升链在此终止.

$(ii) \Rightarrow (iii)$ 由选择公理, 显然成立.

$(iii) \Rightarrow (i)$ I 为任意理想,$\sum = J \subset I|J$. 由 (iii),$\sum$ 有极大元, 设为 J_0. 但是 $J_0 = I$, 否则任意 $f \in J_0$ 可给出理想 $J_0 + Af$, 它是有限生成的但比 J_0 大.

请证明 $\mathbb{Z}$ 和 $k[X]$ 是诺特环.

3.2 命题

(i)A 为诺特环,$I \subset A$ 为理想, 那么商环 B=A/I 为诺特环.

(ii) 令 A 为诺特整环,$A \subset K$ 为分式域,$0 \notin S \subset A$ 是子集, 令

$$B = A[S^{-1}] = a/b \in K|a \in A,\ b = 1\ \ S \quad .$$

证明参考 3.4.

3.3 希尔伯特基定理

环 A 有,

$$\text{A 是诺特环 } \Rightarrow \text{A[X] 是诺特环.}$$

证明 令 $J \subset A[X]$ 是任意理想, 证明 J 有限生成. 定义首项为 n 次的 J 的元素为

$$J_n = a \in A | \exists f = aX^n + b_{n-1}X^{n-1} + .. + b_0 \in I.$$

那么 J_n 是 A 的理想而且 $J_n \subset J_{n+1}$. 因此, 由升链条件, 存在 N 使 $J_N = J_{N+1} = ...$

建立 J 的生成元集: 对于 $i \leqslant N$, 令 $a_{i1}, ..., a_{im(i)}$ 为 J_i 的生成元, 在 J_i 的定义里, 对每个 a_{ik}, 令 $f_{ik} = a_{ik}X^i + ... \in J$ 为 i 次首项为 a_{ik} 的元素.

下证集

$$f_{ik} | i = 0, ..., N, k = 1, ..., m(i)$$

生成 J: 对给定的 $g \in J$, 假定 $\deg g = m$. 那么 g 的首项为 bX_m,$b \in J_m$. 有 $b = \sum c_{m'k}a_{m'k}$($m' = m$ $m \leqslant N$, $m' = N$). 然后考虑 $g_1 = g - X^{(m=m')}\sum c_{m'k}f_{m'k}$: 通过构造可使 m 次数为 0, 所以 $degg_1 \leqslant degg - 1$; 最终可写出 g 由 f_{ik} 组合而成的形式, 所以生成 J.

推论 若 k 为域, 那么有限生成 k 代数为诺特环.

有限生成 k 代数是一个形如 $A = k[a_1, ..., a_n]$ 的环, 所以 A 是由 k 与 $a_1, ..., a_n$ 有限生成的环. 很明显, 每个这样的环都同构于一个多项式环的商环,$A \backsimeq k[a_1, ..., a_n]/I$. 域是诺特环, 由 (3.3),$k[a_1, ..., a_n]$ 是诺特环, 最后由 (3.2)(i) 商环也是诺特环.

3.4 对应 V

k 是任意域,$A = k[a_1, ..., a_n]$. 记 $\mathbb{A}_k^n = k_n$ 为 k 上 n 维仿射平面.$k(a_1, ..., a_n) \in A$ 点 $P = (a_1, ..., a_n) \in \mathbb{A}_k^n = k_n$,$f(a_1, ..., a_n) \in k$. 定义对应 V

$$\begin{aligned} J \subset A &\longrightarrow \quad X \in \mathbb{A}_k^n \\ J &\longmapsto V(J) = P \in \mathbb{A}_k^n | f(P) = 0 \quad f \in J \end{aligned}$$

定义 子集 $X \subset \mathbb{A}_k^n$ 是代数集如果 X=V(I) 对某些 I 成立. 由 3.3,I 为有限生成的. 如果 $I = (f_1, ..., f_r)$ 那么显然

$$VI = P \in \mathbb{A}_k^n | f_i(P) = 0, i = 1, .., r$$

所以代数集是满足一个多项式方程的有限点的轨迹.

若 I=(f) 是主理想, 那么通常把 V(I) 写成 V(f).

3.5 命题与定义

对应 V 满足:

$(i)V(0)=\mathbb{A}_k^n; V(A)=\phi$;

$(ii)I\subset J\Rightarrow V(I)\supset V(J)$;

$(iii)V(I_1\bigcap I_2)=V(I_1)\bigcup(I_2)$;

$(iv)V(\sum_{\lambda\in\Lambda}I_\lambda)=\bigcap_{\lambda\in\Lambda}V(I_\lambda)$

因此 $\mathbb{A}_k^n$ 的代数集构成了 $\mathbb{A}_k^n$ 上拓扑的闭集,Zariski 拓扑.

只给出 (iii) 的 $\subset$ 的证明. 设 $P\notin V(I_1)\bigcup(I_2)$, 有 $f\in I_1, g\in I_2$ 使得 $f(P)\neq 0, g(P)\neq 0$. 所以 $fg\in I_1\bigcap I_2$, 但 $fg(P)\neq 0$, 因此 $P\notin V(I_1\bigcap I_2)$.

3.6 对应 I

V 的某种逆, 有对应 I

$$J\subset A\longleftarrow\quad X\subset\mathbb{A}_k^n$$
$$I(X)=f\in A|f(P)=0,\ \ P\in X\leftarrow X$$

这意味着 I 把 X 映成在 X 上为 0 的函数.

命题 (a)$X\subset Y\Rightarrow I(X)\supset I(Y)$;

(b) 对任意子集 $X\subset\mathbb{A}_k^n$, 有 $X\subset V(I(X))$ 当且仅当 X 为代数集;

(c) 对 $J\subset A$, 有 $J\subset I(V(J))$; 为严格包含.

证明 (a) 显然.(b) 与 (c) 的包含为同义反复的:I(X) 被定义为在 X 上所有点为 0 的函数集, 那么对于 X 中一点, 所有 I(X) 中函数在其上为 0.

(b) 中剩下的部分很简单: 若 X=V(I(X)) 那么 V 是代数集, 因为它为形式 V(某理想). 相反地, 如果 $X=V(I_0)$ 是代数集, 那么 I(X) 至少包含 I_0, 故 $V(I(X))\subset V(I_0)=X$.

有两种可能使 (c) 中的包含为严格的.

例 1 假设 k 不是代数闭的, 令 $f\in k[X]$ 为一个非常数多项式, 且在 k 中没有根. 考虑理想 $J=(f)\subset k[X]$. 那么 $J\neq k[X]$, 因为 $1\notin J$. 但

$$V(J)=P\in\mathbb{A}_k^1|f(P)=0=\phi$$

因此 I(V(J))=k[X].

所以如果域不是代数闭的, 可能无法有足够的零点. 一个相似的例子: 在 $\mathbb{R}^2$, 多项式 X^2+Y^2 定义了单点 $P=(0,0)$, 故 $V(X^2+Y^2)=P$. 但是除此之外还有很多在 P 为 0 的多项式, 而且事实上 I(P)=(X,Y).

例 2 对任何 $f\in k[X_1,...X^2]$ 且 $a\geqslant 2$,f^a 定义了与 f 相同的轨迹,$f^a(P)=0\iff f(P)=0$. 所以 $V(f^a)=V(f)$, 且 $f\in I(V(f^a))$, 但是通常 $f\notin(f^a)$. 在例 1 中, 讨论的是 $X^2=0$ 定义的两条直线, 它只能意味着 (X=0) 平方了, 但事实并非如此.

3.7 不可约代数集

一个代数集 $X \subset \mathbb{A}_k^n$ 是不可约的, 如果不存在分解

$$X = X_1 \cup X_2 \; X_1, X_2 \subsetneq X$$

比如, 代数集 $V(xy) \subset \mathbb{A}_k^n$ 是由两坐标轴组成的轨迹, 显然是 V(x) 与 V(y) 的组合, 所以是可约的.

命题 (a) 令 $X \subset \mathbb{A}_k^n$ 是代数集且 I(X) 是对应的理想. 那么

$$\text{X 是不可约的} \iff \text{I(X) 是素理想.}$$

(b) 任何代数集 X 有唯一分解

$$X = X_1 \cup ... \cup X_r \tag{*}$$

X_i 不可约且 $X_i \nsubseteq X_j$ 当 $i \neq j$.

证明 (a) 要证 X 是不可约的 $\iff$ I(X) 不是素的.

($\Rightarrow$) 设 $X = X_1 \cup X_2$,$X_1 \nsubseteq X$ 意味着有 $f_1 \in I(X_1)/X$, 相似地 $X_2 \nsubseteq X$ 意味着有 $f_2 \in I(X_2)/X$.$f_1 f_2$ 在 X 的所有点上为 0, 故 $f_1 f_2 \in I(X)$. 则 I(X) 不是素的.

($\Leftarrow$) 设 I(X) 不是素的, 有 $f_1, f_2 \notin I(X)$ 使 $f_1 f_2 \in I(X)$. 让 $I_1 = (I(X), f_1)$ 且 $V(I_1) = X_1$, 那么 X 的真子集 X_1 为代数集. 同理, 得到 X_2. 由 $X \subset X_1 \cup x_2$, 对任意 $P \in X$,$f_1 f_2(P) = 0$ 意味着 $f_1(P) = 0$,$f_2(P) = 0$.

(b)$\mathbb{A}_k^n$ 中代数集构成链

$$X_1 \supset X_2 \supset ... \supset X_n \supset ...$$

最终终止. 这是因为

$$I(X_1) \subset I(X_2) \subset ... \subset I(X_n) \subset ...$$

是 A 的理想构成的升链. 正如在 3.1 中,

$$\mathbb{A}_k^n \text{ 上代数集的任何非空 } \sum \text{ 有极小元.} \tag{!}$$

令 $\sum$ 为 $\mathbb{A}_k^n$ 的代数子集, 它没有分解 (*). 若 $\sum = 0$ 那么 (b) 成立, 否则, 由 (!), 必有极小元 $X \in \sum$, 这样有: 若 X 不可约, 那么 $X \notin \sum$, 矛盾; 若 X 可约, 那么 $X = X_1 \cup x_2$,X_1, X_2 为 X 的真子集. 又 X 为极小元,$X_1, X_2 \nsubseteq \sum$. 所以 X_1, X_2 各有分解 (*), 把它们合并有 (*) 的分解, 故 $X \notin \sum$. 所以 $\sum = 0$.(b) 得证.

3.8 断言

让 k 为有限域,$A = k[a_1, ..., a_n]$ 是有限生成 k 代数. 那么

$$\text{A 是数域} \Rightarrow \text{A 在 k 上是代数的}$$

粗略证明: 若 $t \in A$ 是 k 上超越元, 那么 k[t] 是多项式环, 有无限多个素元. 因此扩张 $k \subset k(t)$ 不是有限生成的 k 代数: 有限多个元素 $p_i/q_i \in k(t)$ 只能有有限多个素的生成元.

3.9 希尔伯特零点定理

假设 k 是一个代数闭域.

(a) 多项式环 $A = k[X_1, \dots X_n]$ 中的极大理想总是有着 $m_P = (X_1 - a_1, \dots X_n - a_n)$ 的形式, 其中 $P = (a_1, \dots a_n) \in \mathbb{A}_k^n$; 也就是说, 极大理想是在 P 处取 0 值的所有函数的理想 $I(P)$.

(b) 如果 $J \subset A$ 是一个理想,$J \neq (1)$, 则 $V(J) \neq \varnothing$.

(c) 对于任意 $J \subset A$,$I(V(J)) = radJ$

定理的必要条件是 (b), 即如果一个理想 J 不是整个环 $k[X_1, \dots X_n]$, 则理想中的多项式就会在 $\mathbb{A}_k^n$ 上有零点. 注意, 如果 k 不是代数闭域, 那么 (b) 就是完全错误的, 因为如果 $f \in k[X]$ 是一个非常数多项式, 那么 f 就不能作为一个理想来生成整个 $k[X]$, 但是可能有 $V(f) = \varnothing \subset \mathbb{A}_k^1$.

推论 对应关系 V 和 I

$$\begin{array}{ccc} \{\text{理想} I \subset A\} & \overset{V,I}{\longleftrightarrow} & \{\text{子集} X \subset A^n k\} \\ \text{导出双射} \quad \cup & & \cup \\ \{\text{根理想}\} & \longleftrightarrow & \{\text{代数子集}\} \\ \text{以及} \quad \cup & & \cup \\ \{\text{素理想}\} & \longleftrightarrow & \{\text{不可约代数子集}\} \end{array}$$

上述双射成立时因为由 (3.6, b) 对任意代数集 X 有 $V(I(X)) = X$, 而由 (3.10, c) 对任意根理想 J 有 $I(V(J)) = J$.

零点定理的证明 (假设 3.8 成立)

(a) 设 $m \subset k[X_1, \dots X_n]$ 是一个极大理想, 取 $K = k[X_1, \dots X_n]/m$, 则有 φ 是两个自然映射的合成 $\varphi : k \to k[X_1, \dots X_n] \to K$. 则 K 是一个域 (因为 m 是极大的), 而作为 k-代数 K 是有限生成的 (因为 K 由 X_i 的象生成). 所以由 (3.8),$\varphi : k \to K$ 是一个代数的域扩张. 但是 k 是代数闭域, 所以 φ 是一个同构.

现在, 对每一个 i,$X_i \in k[X_1, \dots X_n]$ 映到一些元素 $b_i \in K$, 所以取 $a_{i=}\varphi^{-1}(b_i)$ 则有 $X_i - a_i \in \operatorname{Ker}\{k[X_1, \dots X_n] \to K\} = m$. 因此这里存在 $a_1, \dots a_n \in k$ 使得 $(X_1 - a_1, \dots X_n - a_n) \subset m$. 另一方面, 左侧显然是一个极大理想, 因此 $(X_1 - a_1, \dots X_N - a_n) = m$. 则 (a) 得证.

$(a) \Rightarrow (b)$ 这一部分证明是简单的. 如果 $J \neq A = k[X_1, \dots X_n]$, 那么对 A 一定存在一个极大理想 m 使得 $J \subset m$ (m 的存在性是显然的, 可以利用升链条件). 由 (a),m 具有形式 $m = (X_1 - a_1, \dots X_n - a_n)$, 则 $J \subset m$ 意味着对于任意 $f \in J$ 有 $f(P) = 0$, 其中 $P = (a_1, \dots a_n)$. 因此 $P \in V(J)$.

$(b) \Rightarrow (c)$ 这一部分需要一个小技巧. 设 $J \subset k[X_1, \dots X_n]$ 是任意理想, 而 $f \in k[X_1, \dots X_n]$. 引入另外一个变量 Y, 考虑由 J 和 $fY-1$ 生成的新理想

$$J_1 = (J, fY-1) \subset k[X_1, \dots X_n, Y]$$

粗略地说,$V(J_1)$ 是一个包含 $P \subset V(J)$ 的簇, 因此 $f(P) \neq 0$. 更准确地说, 一点 $Q \in V(J_1) \subset \mathbb{A}_k^{n+1}$ 是一个 $n+1$ 元 $Q = (a_1, \dots a_n, b)$ 使得

$$\text{对所有} g \in J \text{有} g(a_1, \dots a_n) = 0, \text{ 即} P = (a_1, \dots a_n) \in V(J)$$

以及

$$f(P) \cdot b = 1, \text{即} f(P) \neq 0 \text{ 且} b = f(P)^{-1}.$$

现在假设对所有 $P \subset V(J)$ 有 $f(P) = 0$, 则显然由上文可得 $V(J_1) = \varnothing$. 因此由 (b) 可推出 $1 \in J_1$, 即存在表示

$$1 = \sum g_i f_i + g_0(fY-1) \in k|X_1, \dots X_n, Y\Big]$$

其中 $f_i \in J$ 而 $g_0, gi \in k[X_1, \dots X_n, Y]$.

考虑为什么上式中 Y 在右侧: 除了显式地表示,Y 还存在在每一个 g_i 中, 假设 Y^N 是 Y 在 g_0, gi 中存在的最高阶. 如果将两边同乘 f^N, 就有关系

$$f^N = \sum G_i(X_1, \dots X_n, fY) f_i + G_0(X_1, \dots X_n, fY)(fY-1)$$

其中 G_i 是 $f^N g_i$ 用 $X_1, \dots X_n$ 和 (fY) 的多项式形式写出来的.

上式是仅关于 $k[X_1, \dots X_n, Y]$ 的多项式的等式, 因此可以两边同模 $(fY-1)$ 得到

$$f^N = \sum h_i(X_1, \dots X_n) f_i \in k[X_1, \dots X_n, Y]/(fY-1)$$

等式两边都是 $k[X_1, \dots X_n]$ 中的元素. 因此自然的同态 $k[X_1, \dots X_n] \hookrightarrow k[X_1, \dots X_n, Y]/(fY-1)$ 是一个内射 (这是 $k[X_1, \dots X_n]$ 到 $k[X_1, \dots X_n][f^{-1}]$ 的一个自然嵌入, 就像子环和它的分式域一样), 它遵循

$$f^N = \sum h_i(X_1, \dots X_n) f_i \in k[X_1, \dots X_n]$$

即对任意 N 有 $f^N \in J$. 则证毕.

3.10 一些实例

(a) 超平面

关于簇的一个最简单实例是超平面 $V(f) : (f = 0) \subset \mathbb{A}^n k$. 如果 k 是代数闭域, 那么在不可约元 $f \in k[X_1, \dots X_n]$ 和不可约超平面上就有一个自然的对应关系: 由零点定理, 两个互质的不可约多项式 f_1, f_2 定义了两个不同的超平面 $V(f_1), V(f_2)$. 这并不总是显然的 (例如, 在 $\mathbb{R}$ 上就不成立), 尽管这不用零点定理而用消去定理 (19 世纪提出的一个更加显式的方法) 就能证明, 即练习 *3.13*.

(b)

除了超平面外, 绝大多数的簇都是由很多等式来定义的. 反直觉地, 这通常都是因为理想 $I(X)$ 有多个生成元, 即多于 X 的共同维数的生成元. 例如, 对于 $C \subset \mathbb{A}^3 k$,$I(C)$ 需要三个生成元, 现在假设 k 是一个无限域.

先考虑,$J = (uw - v^2, u^3 - vw)$. 其中 J 不是素的, 因为

$$J \ni w\left(uw - v^2\right) - v\left(u^3 - vw\right) = u\left(w^2 - u^2 v\right)$$

而 $u, w^2 - u^2 v \notin J$. 因此

$$V(J) = V(J, u) \cup V\left(J, w^2 - u^2 v\right)$$

显然,$V(J, u)$ 是直线 $(u = v = 0)$. 同时, 另外一部分 $C = V\left(J, w^2 - u^2 v\right)$ 是一个不可约曲线, 而 C 由三部分给出:

$$uw = v^2, u^3 = vw, w^2 = u^2 v$$

现在证明 $C \subset \mathbb{A}^3$ 是映射 $\varphi : A^1 \to C \subset A^3$ 在 $t \mapsto t^3, t^4, t^5$: 下的象: 如果 $u \neq 0$ 则 $v, w \neq 0$. 取 $t = v/u$, 则 $t = w/v/$ 且 $t^2 = (v/u)(w/v) = w/u$. 因此 $v = w^2/u^2 = t^4, u = v/(v/u) = t^4/t = t^3/$ 并且 $w = tv = t^5$, 则 C 是不可约的, 因此如果 $C = X_1 \cup X_2, X_i \subset C$, 且 $f_i(u, y, w) \in I\left(X_i\right)$, 则对于所有 t, 至少有一个 $f_i\left(t^3, t^4, t^5\right)$ 取到 0 值. 因为一个非零多项式至多有有限个零点, f_1, f_2 中的一个必须为 0, 所以 $f_i \in I(C)$.

这个实例是一个不错的单项式的例子, 通常情况下是很难找到一个簇的不可约部分的, 更别提证明它不可约了. 一个同样的例子为练习 *3.11*

3.11 有限代数

现在开始证明 (3.8). 设 $A \subset B$ 都是环. 通常来说, 如果存在有限个元素 $b_1, \ldots b_n$ 使得 $B = A\left[b_1, \ldots b_n\right]$, 则 B 被称作在 A 上的有限扩张 (或 $A-$ 代数), 因此 B 由 A 和 $b_1, \ldots b_n$ 生成.

与下述定义做对比: 如果存在有限个元素 $b_1, \ldots b_n$ 使得 $B = Ab_1 + ..Ab_n$, 则 B 被称作有限 $A-$ 代数, 即,B 作为 $A-$ 模是有限生成的.

两个定义最大的不同是一个是作为环 (即允许对 b_i 的任意多项式表达), 一个是作为模 (只允许线性表达). 例如,$k[X]$ 是一个有限生成 $k-$ 代数 (仅由一个元素 X 生成), 但这不是一个有限 $k-$ 代数 (因为作为 $k-$ 向量空间它是无限维的).

命提 (i) 设 $A \subset B \subset C$ 都是环: 则

$$B\text{是}A - \text{代数且}C\text{是有限}B - \text{代数}$$
$$\Rightarrow C\text{是有限}A - \text{代数}$$

(ii) 如果 $A \subset B$ 是一个有限 A-代数且 $x \in B$ 则 x 满足一个在 A 上的首一多项式, 即存在关系

$$x^n + a_{n-1}x^{n-1} + ..a_0 = 0\text{其中}a_i \in A$$

(注意其中首项系数是 1).

(iii) 反过来, 如果 x 满足一个在 A 上的首一多项式, 则 $B = A[x]$ 是一个有限 $A-$ 代数.

证明 (i) 和 (iii) 简单的 (仿照域扩张的相似结论). 对于 (ii), 可以使用一个不太显然的行列式技巧: 假设 $B = \sum Ab_i$; 则对于任意 $i, xb_i \in B$, 所以有常数 $a_ij \in A$ 使得

$$xb_i = \sum_j a_{ij} b_j$$

也可以写作

$$\sum_j \left(x\delta_{ij} - a_{ij}\right) b_j = 0$$

其中 δ_{ij} 是单位矩阵. 则设 M 是矩阵:

$$M_{ij} = \left(x\delta_{ij} - a_{ij}\right)$$

然后取 $\Delta = \det M$. 然后由标准线性代数, (将 b 写作列向量和项 $(b_1, \dots b_n)$ 以及 M 的伴随矩阵 $M^a dj$).

$$Mb = 0, \quad \text{因此} \quad 0 = \left(M^{adj}\right) Mb = \Delta b$$

则对所有 i 有 $\Delta b_i = 0$. 但是, $1_B \in B$ 是关于 b_i 的线性组合, 因此 $\Delta = \Delta \cdot 1B = 0$, 最后则得到关系: $\det\left(x\delta_{ij} - a_{ij}\right) = 0$. 则显然有对 x 的首一多项式, 而系数则来自 A.

3.12 诺特正规化

诺特正规化引理 设 k 是一个无限域, 同时 $A = k\left[a_1, \dots a_n\right]$ 是一个有限生成的 k -代数. 则存在 $m \leq n$ 和 $y_1, ..y_m \subset A$ 使得

(i) $y_1 \dots y_m$ 在 k 上代数独立;

(ii) A 是有限 $k\left[y_1, \dots y_m\right]$ -代数.

((i) 意味着对 y_i 的线性组合, 当且仅当系数全为 0 时才取到 0 值; 代数地来讲, 就是自然的映射 $k\left[Y_1, \dots Y_m\right] \to k\left[y_1, \dots y_m\right] \subset A$ 是单射.

可以断言, 环的扩张可以通过首先引入代数独立的元素, 然后“进行代数扩张”来建立. 但是, (ii) 远比此精确得多, 因为它说 A 中的每个元素不仅是在 $k\left[y_1, \dots y_m\right]$ 上代数的, 还满足在其上的首一多项式.

证明 取 I 是自然满射的核

$$I = \ker\left\{k\left[X_1, \dots X_n\right] \to k\left[a_1, \dots, a_n\right] = A\right\}$$

假设 $0 \neq f \in I$; 证明的思路是将 $X_1 \dots X_{n-1}$ 替换为确定的 $X_1' \dots X_{n-1}'$ 使得 f 对于 a_n 在 $A' = k\left[a_1', \dots a'n - 1\right]$ 上是一个首一多项式.

所以记

$$a_1' = a_1 - c_1 a_n$$
$$\dots$$
$$a_{n-1}' = a_{n-1} - a_{n-1} a_n$$

(其中 α_i 是 k 中的元素). 之后有

$$0 = f\left(a'1 + \alpha_1 a_n, \ldots\right) a'_{n-1} + \alpha_{n-1} a_n, a_n\big)$$

断言 选择合适的 $\alpha_1, \ldots \alpha_{n-1} \in k$, 则多项式

$$f\left(X'_1 + \alpha_1 X_{n,w}, X^*_{n-1} + \alpha_{n-1} X_n, X_n\right)$$

是关于 X_n 的首一多项式.

利用上述断言, 可以通过归纳法证明该引理: 当 $n = 1$ 时是显然的; 当 $n = n$ 时, 若 $I = 0$, 则显然, 因为 $a_1, \ldots a_n$ 是代数独立的. 其他情况下, 取 $0 \neq f \in I$, 和 $n = n - 1$ 时的 $\alpha_1, \ldots \alpha_{n-1}$; 则 f 给出了一个满足 a_n 的首一多项式, 其中系数来自 $A' = k\left[a'_1, \ldots a'n - 1\right] \subset A$. 由归纳假设, 存在 $y_1, \ldots y_m \in A'$ 使得

(1) $y_1 \ldots y_m$ 在 k 上时代数独立的;

(2) A' 是有限 $k\left[y_1, \ldots \text{ y } m\right]$ -代数.

则 $A = A'\left[a_n\right]$ 在 A' 上是有限扩张 (由 (3.12.*iii*)), 因此由 $(3.12, i)$, A 在 $k\left[y_1, \ldots y_m\right]$ 上是有限扩张, 证毕.

最后剩下来的是断言的证明. 取 $d = \deg f$, 并设

$$f = F_U + G$$

其中 F_d 是 d 次齐次多项式, 另外 $\deg G \leq d - 1$. 则

$$\begin{aligned} f\left(X_1, \ldots X_{n-1}, X_n\right) &= f\left(X'_1 + \alpha_1 X_{n,}, \ldots, X'_{n-1} + \alpha_{n-1} X_n, X_n\right) \\ =& F_d\left(\alpha_1, \ldots \alpha_{n-1}, 1\right) \cdot X_n^d + \left(\text{对} X_n \text{的阶数} \leq d-1 \text{的部分}\right) \end{aligned}$$

根据假设有 $F_d\left(\alpha_1, \ldots \alpha_{n-1}, 1\right) \neq 0$. 因为 F_d 是非零多项式, 这就不难验证这是 $\alpha_1, \ldots \alpha_{n-1}$ 在几乎所有取值的情况 (进一步的证明在练习 *3.13*). 则证毕.

3.13 注

(I) 事实上,(3.13) 的证明表示可以选择足够好的 $y_1 \ldots y_m$ 使得是对 $a_1, \ldots a_n$ 的 m 一般线性形式. 为了理解 (3.13), 记 $I = \ker\left\{k\left[X_1, \ldots X_n\right] \to k\left[a_1, \ldots a_n\right] = A\right\}$, 并且假设 I 是素的. 考虑 $V = V(I) \subset \mathbb{A}^n k$; 并设 $\pi : \mathbb{A}^n k \to \mathbb{A}^m k$ 是由 $y_1, \ldots y_m$, 和 $p = \pi | v : V \to \mathbb{A} m_k$ 定义的线性投影. 这就可以看出 (3.13) 的结论 (i) 和 (ii) 意味着在每一个 $P \in \mathbb{A}^m k$ 上, $p^{-1}(P)$ 是一个无限非空集 (即练习 *3.16*).

(II)(3.13) 的证明也有一个简单的几何解释: 从 n 个变量 $X_1, \ldots X_n$ 中选取 $n - 1$ 个线性形式对应于构造一个线性投影 $\pi : \mathbb{A}_k^n \to \mathbb{A}_k^{n-1}$; π 中的线条就构成了一个 $(n-1)-$ 维平行线簇. 选取多项式 $f \in I$, 就不难看出当且仅当没有一个平行线的渐近线是 $(f = 0)$ 则 f 给出了一个关于最后的 X_n 的首一多项式; 在射影几何中, 这意味着无穷远点 $(0, \alpha_1, \ldots \alpha_{n-1}, 1) \in \mathbb{P}_k^{n-1}$ 代表着平行投影不属于 $(f = 0)$ 上的射影闭集.

(III) 上面关于 (3.13) 的证明在有限域上并不成立 (即练习 *3.14*). 但是定理本身是不需要任何关于 k 的条件的.

3.14 (3.8) 的证明

$A = k[a_1, \dots a_n]$ 是一个有限生成的 k -代数. 假设 $y_1, \dots y_m \in A$ 满足 (3.13) 中的条件, 并记 $B = k[y_1, y_m]$. 则 A 是一个有限 B -代数, 已知 A 是一个域. 若 B 是一个域, 那么就有 $m = 0$, 使得 A 是一个有限 k -代数, 即,k 的一个有限域扩张,(3.8) 则得证. 因此仅需证:

引理 若 A 是一个域, 同时 $B \subset A$ 是一个子环使得 A 是一个有限 B -代数, 那么 B 就是一个域.

证明 对任意 $0 \neq b \in B$, 它的逆 $b^{-1} \in A$ 在 A 中. 则由 (3.12 的 ii). b^{-1} 对于 B 有一个首一多项式, 即存在关系

$$b^{-n} + a_{n-1}b^{-(n-1)} + \dots a_1 b^{-1} + a_0 = 0, \quad \text{其中} a_i \in B$$

两边同乘 b^{n-1}

$$b^{-1} = -\left(a_{n-1} + a_{n-2}b + \dots a_0 b^{n-1}\right) \in B$$

因此 B 是一个域. 这就证明了 (3.8) 并完成了零点定理的所有证明.

3.15

为了让上述证明在特征 p 的域上是成立的, 在这里做一些调整使其更普适. 这一段会用到伽罗瓦理论的分离性内容, 如果对此毫无头绪可以略过本段.

附录 在 (3.13) 的条件下, 如果更进一步设 k 是代数闭的, 且 A 是一个整环并且有分式域 K, 那么就可以像上面一样挑出 $y_1, \dots y_m \in A$ 满足 (i) 和 (ii), 并且另外满足条件 (iii) $k(y_1, \dots y_m) \subset K$ 是一个可分扩张.

证明 如果 k 是特征 0 的, 那么所有域扩张都是可分扩张; 假设 k 是特征 p 的. 因为 A 是一个整环,I 是素的; 因此如果 $I \neq 0$, 那么它就包含一个不可约元 f. 现在对任意 i 这里有两种情况: 要么 t 在 X_i 上是可分的, 要么有 $f \in k\left[X_1, \dots X_i^P, \dots X_n\right]$.

断言 如果 f 在每一个 X_i 上都不可分, 那么 $f = g^P$, 与 f 的不可分性冲突.

假设 f 具有形式:

$$f = F\left(X_1^D, \dots X_n^D\right), \text{其中} F \subset k[X_1, \dots X_n]$$

设 $g \in k[X_1, \dots X_n]$ 是取系数为 F 的第 p 个根所做成的多项式, 然后重复使用在特征 p 上的恒等式 $(a+b)P = aP + bP$, 这就容易看出 $f = g^P$.

因此任意不可约的 f 至少在一个 X_i 中是可分的, 不妨设为 X_n. 然后就像上文一样, 有

$$f\left(X_1' + \alpha_1 X_n, \dots X_{n-1}' + \alpha_{n-1}X_n, X_n\right)$$

这是一个首一多项式, 这个可分关系是在 $A' = k\left[a_1', \dots a_{n-1}'\right]$ 上对 a_n 成立的. 最后, 由相同的归纳可以证明, 可分域扩张的合成依然是可分的. 则得证.

3.16 降至超平面

在伽罗瓦理论中, 有以下结论

本原元定理. 设 K 是一个无限域, 且 $K \subset L$ 是一个有限可分的域扩张; 那么就存在 $x \in L$ 使得 $L = K(x)$. 进一步, 如果 L 是在 K 上由元素 $z_1, \dots z_k$ 生成的, 那么 x 可以通过 z_i 的线性组合即 $\sum_i \alpha_i z_i$ 表出.

(下列是来自伽罗瓦理论的基本定理: 如果 $K \subset M$ 是 L 在 K 上的正规闭包则 $K \subset M$ 是一个有限伽罗瓦域扩张, 因此由基本定理在 K 和 M 间只存在有限个中间域扩张. 而在 K 和 L 间的中间子域构成了一个有限集 $\{K_j\}$, 这个有限集是关于 L 的一个 K -向量子空间, 因此可以选出 $x \in L$ 而不在任意一个中间子域中. 如果已经给出 $z_1, \dots z_k$, 并且不是全部都属于任意 K_i, 则 x 可以作为对 z_i 的 K -线性组合而表出. 最后则有 $K(x) = L$.)

推论 在诺特正规化引理 (3.13) 的假设下, 存在 $y_1 \dots y_{m+1} \in A$ 使得 $y_1 \dots y_m$ 满足 (3.13) 的结论, 另外还有 A 的分式域 K 是在 k 上由 $y_1, \dots y_{m+1}$ 生成的.

证明 根据 (3.16), 可以取 K 是 $k(y_1, \dots y_m)$ 的可分扩张. 如果 $A = k[x_1, \dots x_n]$, 则有 x_i 确实地生成 K, 使其作为一个 $k(y_1, \dots y_m)$ 上的域扩张, 所以对 y_{m+1} 存在一个合适的, 关于 x_i 的, 且系数都来自 $k(y_1, \dots y_m)$ 的线性组合来生成这个域扩张; 如果将线性组合中的分母消去, 那么组成 y_{m+1} 的线性组合就变成关于 x_i 的, 且系数都来自 $k[y_1, \dots y_m]$ 的, 因此 y_{m+1} 是 A 中的一个元素. 则得证.

代数地来讲, 上面的证明是说, 一个不纯粹超越的域扩张 $k \subset K$, 可以作为纯粹超越的域扩张 $k \subset k(y_1, \dots y_m) = K_0$ 和一个初等的代数域扩张 $K_0 \subset K = K_0(y_{m+1})$ 的合成. 也就是说, $K = k(y_1, ..y_{m+1})$, 对生成元而言只有一个代数的依赖关系. 而在几何上的意义将会在 (5.10) 中解释清楚.

练习

习题 3.1　取 $f = X^2 - Y^2$ 及 $g = X^3 + XY^2 - Y^3 - X^2Y - X + Y$; 找出 $V(f, g) \subset \mathbb{A}^2_{\mathbb{C}}$ 的不可约成分.

解：显然 $f = (X - Y)(X + Y), g = (X - Y)(X^2 + Y^2 - 1)$.

因此取 $J = (f, g)$ 则有 $J \in (X+Y)*f-1*g = (X-Y)(1+2XY)$, 其中 $X-Y, 1+2XY \notin J$, 因此 $V(J) = V(J, X - Y) \cup V(J, 1 + 2XY)$.

显然,$V(J, X - Y)$ 是直线 $(X = Y)$, 同时另外一部分 $C = V(J, 1 + 2XY)$ 是一个不可约曲线. 因此 $V(f, g) \subset \mathbb{A}^2_{\mathbb{C}}$ 的不可约成分为 $C = V(f, g, 1 + 2XY)$

习题 3.2　若 $J = (uw - v^2, w^3 - u^5)$, 证明 $V(J)$ 有两个不可约成分, 并且其中之一是 (3.11,b) 中的曲线 C.

证明同一个曲线 C 可以由两个方程给出:$uw = v^2$ 和 $u^5 - 2u^2vw + w^3 = 0$. 这个问题的重点是第二个方程, 受限于二次曲线 $(uw = v^2)$ 它必须是一个完全平方形式.

解:

习题 3.3 取 $f = v^2 - uw.g = u^4 - vw.h = w^2 - u^3v$. 类似 (3.11,b), 分解 $V(f,g,h) \subset A^3$. 并考虑 $V(f,g), V(f,h)$和$V(g,h)$ 有没有其他的成分.

习题 3.4 举例说明 (3.13) 关于诺特正规化引理的证明在有限域 k 上不成立.(提示: 对 $F_d(\alpha,1) = \alpha^q - \alpha$ 找出多项式 $f(X,Y)$, 使得对于所有 $\alpha \in k$ 有 $F_d(\alpha,1) = 0$

Chapter 4

仿射簇上的函数

在这个部分我在一个固定的域上讨论；从 $(4.8, ii)$ 开始, 假设 k 是代数闭的. 读者可以假设 k=C, 有时为简化表示法, 会省略对域 k 的提及.

4.1 多项式函数

如果 $V \subset A_k^n$ 是一个代数集, I(V) 是它的理想, 那么称商环 $k[V] = k[X_1, X_2 \cdots, X_n]/I(V)$ 为 V 上的函数环. 更详细地说, 把 V 上的多项式函数定义成映射 $f : V \to k, P \mapsto F(P)$, 其中 $F \in k[X_1, X_2 \cdots, X_n]$, 这就意味着 f 是多项式映射 $F : V \to k$ 限制在 V 上, 由 I(V) 的定义只知, 两个元素 $F, Gk[X_1, X_2 \cdots, X_n]$ 在 V 上定义相同的函数当且仅当

$$F(P) - G(P) = 0, \forall P \in V$$

也就是说当且仅当 $F - G \in I(V)$. 因此可以定义坐标环 k[V],

$$\text{k[V]=\{f: V} \to \text{k| f 是多项式函数 }\} \cong k[X_1, X_2 \cdots, X_n]/I(V)$$

这是 V 上包含坐标函数 X_i 和 k 的最小函数环.

4.2 k[V] 和 V 上的代数子集

一方面, 一个代数集 $X \subset V \subset A^n$; 另一方面, $k[X_1, X_2 \cdots, X_n]$ 中包含 I(V) 的理想和 $k[X_1, X_2 \cdots, X_n]/I(V)$ 中的理想一一对应 (考虑理想 J,$I(V) \subset J \subset k[X_1, X_2 \cdots, X_n]$, 对应 J/I(V); 反过来,$k[X_1, X_2 \cdots, X_n]/I(V)$ 的理想 J_0 对应它在 $k[X_1, X_2 \cdots, X_n]$ 中的原象.)

因此有和第 3 节一样 I 对应和 V 对应, 并有相似的性质.

$$\{ \text{理想 } I \subset k(V)\} \xrightarrow{V} \{ \text{子集 } X \subset V\}$$
$$I \longmapsto V(I) = \{P \in V | f(P) = 0, \forall f \in I\}$$

和

$$\{ \text{子集 } X \subset V\} \xrightarrow{I} \{ \text{理想 } J \subset k(V)\} f$$
$$X \longmapsto I(X) = \{f \in k(V) | f(P) = 0, \forall P \in X\}$$

V 上有 Zariski 拓扑, 其中闭集是代数子集 (这是 A^n 上的 Zariski 拓扑的子拓扑).

定理 $V \subset A^n$ 是代数子集, 下面的条件是等价的:

(i)V 是不可约的;

(ii) 任意两个非空开集 $\emptyset \neq U_1, U_2 \subset V$ 都有 $U_1 \cap U_2 \neq \emptyset$

(iii) 任意非空开集 $U \subset V$ 是稠密的.

V 不可约意味着 V 不是两个非空闭集的并集,(ii) 是 (i) 的一个重述, 因为

$$U_1 \cap U_2 = \emptyset \Longleftrightarrow V = (V - U_1) \cup (V - U_2)$$

拓扑空间是稠密的当且仅当它与每个开集都相交, 所以 (iii) 是二的一个重述.

4.3 多项式映射

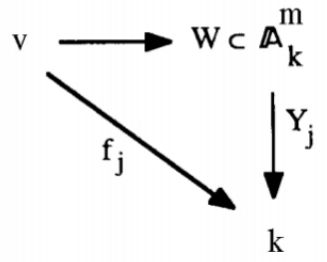
$V \subset A^n, W \subset A^m$ 是代数集,$X_1, \cdot, X_n$ 和 $Y_1, \cdot, Y_m$ 分别是 A^n, A^m 的坐标

定义 称一个映射 f:V ⇒W 是多项式映射, 如果存在 m 个多项式 $F_1, F_2 \cdots, F_m \in k[X_1, X_2 \cdots, X_n]$, 满足

$$f(P) = (F_1(P) \cdots, F_m(P)), \forall P \in V$$

这显然是上面多项式函数的推论.

声明 一个映射 f:V ⇒W 是多项式映射当且仅当 $\forall j, f_j = Y_j \circ f \in k[V]$, 其中 Y_j 是第 j 个坐标函数.



" $\Longrightarrow$ " 如果 f 是由 $F_1 \cdots, F_m$ 定义的, 那么复合映射就是 $P \to F_j(P)$, 是一个多项式函数.

" $\Longleftarrow$ " 如果 $\forall j, f_j \in k[V]$, 那么可以在满足 $f_j = F_j mod I(v), F_j \in k[X_1, X_2 \cdots, X_n]$ 的 F_j 中选一个, 就得到了 f 的一种定义 $(F_1, F_2 \cdots, F_m)$

由这个声明可知, 映射 f 可写成 $f = (f_1, f_2 \cdots, f_m)$.

多项式映射的复合是由简单的方式定义: 如果 $V \subset A^n, W \subset A^m, U \subset A^l$ 是代数集, 且 f:V →W, g:W →U 是多项式映射, 那么 $g \circ f : V \to U$ 仍然的一个多项式映射; 如果 f 是由 $F_1 \cdots, F_m \in k[X_1, X_2 \cdots, X_n]$ 定义的且 g 是由 $G_1 \cdots, G_m \in k[Y_1, Y_2 \cdots, Y_m]$ 定义, 那么 $g \circ f$ 由 $G_1(F_1 \cdots, F_m) \cdots, G_l(F_1 \cdots, F_m) \in k[X_1, X_2 \cdots, X_n]$ 定义

定义 称代数集之间的多项式映射 f:V →W 是同构, 如果存在多项式映射 g:W →V 使 $g \circ f = id_V, f \circ g = id_W$

几个多项式映射的例子:(2.1) 中的参数化 $R^1 \to C \subset R^2, t \to (t^2, t^3)$ 或者 $(t^2 - 1, t^2 - t)$, (3.11,b) 中讨论的映射 $k \to C \subset A^3_k, t \to (t^3, t^4, t^5)$ 都是多项式映射. 并且, 在讨论诺特正规化

定理时, 考虑一个代数集 $V \subset A_k^n$ 和由 m 个 $Y_1, Y_2 \cdots, Y_m$ 的线性形式定义的映射 $p : V \to A_k^m$, 因为 Y_i 是 X_i 的线性形式, 所以这是多项式映射.

4.4 多项式映射和 k[V]

定理 $V \subset A^n, W \subset A^m$ 是代数集.

(I) 一个多项式映射 f:V →W 导出一个环同态 $f^* : k[W] \to k[V]$, 是由复合函数定义的, 即如果 $g \in k[W]$ 是多项式函数, 那么 $f^*(g) = g \circ f$, 并且 $g \mapsto g \circ f$ 定义了一个环同态, 事实上是一个 k—代数同态 $f^* : k[W] \to k[V]$.

(II) 反过来, 任意一个 k—代数同态 $\Phi : k[W] \to k[V]$ 都是由一个多项式映射 f:V →W 唯一定义的, 即 $\Phi = f^*$.

因此 (I) 和 (II) 表明

$$\{ \text{多项式映射 } f : V \to W\} \longrightarrow \{\text{k-代数同态 } \Phi : k[W] \to k[V]\}$$
$$f \longmapsto f^*$$

是双射.

(III) 如果 f:V →W 和 g:W →U 是多项式应映射, 那么两个环同态可复合 $(g \circ f)^* = f^* \circ g^* : k[U] \to k[W]$

证明 (I) 通过 (4.3), $f^*(g)$ 是多项式映射 $V \to k$, 因此 $f^*(g) \in k[V]$. 显然 $f^*(a) = a, \forall a \in k$(这里把 k 看做 V,W 上的常值函数). 最后 f^* 是环同态是形式上的, 因为 k[W] 和 k[V] 是函数环.(环结构是由点态定义的, 例如,$g_1, g_2 \in k[W]$, 它们的和 $g_1 + g_2$ 也是定义在 W 上是函数且 $(g_1 + g_2)(P) = g_1(P) + g_2(P) \forall P \in W$; 所以 $f^*(g_1 + g_2)(Q) = (g_1 + g_2)(f(Q)) = g_1(f(Q)) + g_2(f(Q)) = f^* g_1(Q) + f^* g_2(Q))$

(III) 可由映射的复合推导出

(II) 的证明需要更多的技巧, 对于 $i = 1, 2 \cdots, m$, 令 $y_i \in k[W]$ 是 W 上的第 i 个坐标函数, 所以

$$k[W] = k[y_1 \cdot, y_m] = k[Y_1, Y_2 \cdots, Y_m]/I(W)$$

现在 $\Phi : k[W] \to k[V]$ 已经给出, 所以可以 $f_i = \Phi(y_i)$ 定义 $f_i \in k[V]$

考虑映射 $f : V \to A_k^m, f(P) = f_1(P) \cdots f_m(P)$, 由于 $f_i \in k[V]$, 所以 f 是多项式映射, 进一步 f 把 V 嵌入到 W 中, 即 $f(V) \subset W$. 事实上, 假设 $G \in I(W) \subset k[Y_1, Y_2 \cdots, Y_m]$; 那么

$$G(y_1 \cdot, y_m) = 0 \in k[W]$$

左边是我把环元素 y_i 代入多项式表达式 G, 所以 $\Phi(G(y_1 \cdot y_m)) = 0 \in k[V]$; 但 k 是 k-代数同态, 所以

$$k[V] \in 0 = \Phi(G(y_1 \cdot, y_m)) = G(\Phi(y_1) \cdot, \Phi(y_m)) = G(f_1 \cdot, f_m)$$

fi 是 V 上的函数, $G(f_1 \cdot f_m) \in k[V]$ 是由函数 $P \mapsto G(f_1(P)) \cdot, f_m(P))$ 定义的. 这证明了对 $P \in V$, 每一个 $G \in I(W), f(P)$ 的坐标 $(f_1(P)) \cdot, f_m(P))$ 满足 $G(f_1(P)) \cdot, f_m(P)) = 0$. 因为 W 是由 $G \in I(W)$ 的零点定义的 A_k^m 的子集, 它满足 $f(P) \in W$. 这证明了上面给出分 f 是多项式映射 f:V →W. 为了检验两个 k-代数同态 $f^*, \Phi : k[W] \to k[V]$ 相符, 只要证明它们的生成元相

同, 即 $f^*(y_i) = \Phi(y_i)$, 从 f 的构造中可以发现这个事实. 一个相似的论证可以表明映射 f 是由 $f^*(y_i) = \Phi(y_i)$ 唯一决定的.

4.5 推论

一个多项式映射 f:V →W 是同构当且仅当 $f^* : k[W] \to k[V]$ 是同构.

例子 k 是无限域, 多项式映射

$$\varphi : A_k^1 \to C : (Y^2 = X^3)T \mapsto (T^2, T^3)$$

不是同构. 因为这种情况下, 同态

$$\varphi^* : k[C] = k[X, Y]/(Y^2 - X^3) \to k[T]$$

是由 $X \mapsto T^2, Y \mapsto T^3$ 给出的.φ^* 的象是由 T^2, T^3 生成的 k-代数,$k[T^2, T^3] \subsetneq k[T]$ 注意到 φ 是双射, 所以有一个逆映射 $\psi : C \to A_k^1$, 如果 X=Y=0, 则 $(X, Y) \mapsto 0$, 否则 $(X, Y) \mapsto Y/X$. 所以 φ 为什么不是同构呢？重点是 C 上的多项式比 A_k^1 上的少.

4.6 仿射簇

k 是一个域, 仿射簇是同构意义下的不可约代数集 $V \subset A_k^n$.

定理 4.4 告诉我们坐标环 k[V] 是 V 的同构类中的不变量. 这样我就可以少用 $V \subset A_k^n$ 周围的空间定义簇；后面提出的仿射簇总是上述意义下的.

定义 k 上的仿射簇是集合 V 和环 k[V], 其中的 k-值函数 $f : V \to k$ 满足

(i)k[V] 是有限生成的 k-代数,

(ii) 从 k[V] 选择一些生成元 $x_1 \cdot, x_n$, 映射

$$V \to A_k^n$$
$$P \mapsto x_1(P) \cdot, x_n(P)$$

把 V 作为不可约代数集嵌入到 A_k^n.

4.7 函数域

V 是仿射簇, 那么 V 的坐标环 k[V] 是整环, 其中的函数是 V 上的 k 值函数.

定义 V 的函数域 k(V) 是分式域,k(V)=k[V] 的商环 Quot(k[V]). 一个元素 $f \in k(V)$ 是 V 上的有理函数；$f \in k(V)$ 是由 f=g/h 定义的, 其中 $g, h \in k[V]$ 且 $h \neq 0$.

先验 f 不是 V 上的函数, 因为在 h 的零点处 f 无定义, 可是 f 在 $P \in V, h(P) \neq 0$ 处有定义, 所以 f 至少是一个“部分定义函数”, 下面介绍一些术语支持这个想法.

定义 $f \in k(V), P \in V$, 称 f 是正则的或者 P 在 f 的定义域内, 如果存在一种表达 f=g/h, 其中 $g, h \in k[V]$ 且 $h(P) \neq 0$.

值得注意的是 k[V] 通常不是 UFD, 所以 $f \in k(V)$ 可能有本质不同的表示法 f=g/h, 见习题 4.9 中的例子.

称

$$dom\ f = \{P \in V | f \text{ 在 P 点正则 }\} \text{ 为 f 的定义域.}$$
$$\text{且 } V, P = \{f \in k(V) | f \text{ 在 P 点正则 }\} = k[V][\{h^{-1} | h(P) \neq 0\}]$$

那么 $V, P \subset k(V)$ 是子环, 是 V 在 P 点的局部环.

4.8 定理

(I)dom f 在 Zariski 拓扑下是稠密的开集.

假设 k 是代数闭域; 那么

(II)$dom\ f = V \iff f \in k[V]$(即多项式函数 = 正则有理函数),

进一步, 对任意的 $h \in k[V]$, 令

$$V_h = V \backslash V(h) = \{P \in V | h(P) \neq 0\}$$

那么 (III)$V_h \subset dom\ f \iff f \in k[V][h^{-1}]$.

证明 定义 $f \in k(V)$ 的分母的理想

$$D_f = \{h \in k[V] | hf \in k[V]\} \subset k[V]$$
$$= \{h \in k[V] | \text{ 存在一个表示 f=g/h, 其中 } g \in k[V] \cup \{0\}$$

从第一行可以看出, D_f 是 k[V] 的理想. 证明:

$$V \backslash dom\ f = \{P \in V | h(P) = 0 \forall h \in D_f\} = V(D_f)$$

所以 $V \backslash dom\ f$ 是 V 的代数集, 因此 $dom\ f = V \backslash V(D_f)$ 是闭集的补集, 所以是 Zariski 拓扑下的开集. dom f 显然是非空的, 所以由推定理 4.2 知是稠密的.

使用零点定理的 (b),

$$domf = V \iff V(D_f) = \emptyset \iff 1 \in D_f \iff f \in k[V]$$

最后,

$V_h \subset dom\ f \iff h$ 在 $V(D_f)$ 上为 0,

使用零点定理的 (c), $\iff h^n \in D_f$, 对某些 n, 即 $f = g/h^n \in k[V][h^{-1}]$

4.9 有理映射

V 是仿射簇

定义 一个有理映射 $f : V \to A_k^n$ 是由有理函数 $f_1 \cdots, f_n$ 部分定义的映射, 即

$$f(P) = (f_1(P) \cdots, f_n(P)) \forall P \in \cap dom\ f_i$$

通过定义,$dom\ f = \cap dom\ f_i$, 称 f 在 P 点是正则的当且仅当 $P \in domf$. 两个仿射簇 $V \subset A^n, W \subset A^m$ 之间的有理映射 $V \to W$ 被定义成有理映射 $f : V \to A^m$, 满足 $f(dom\ f) \subset W$.

在 (4.3) 的结尾有两个有理映射的例子.

4.10 有理映射的复合映射

有理映射 f:V →W 和 g:W →U 的复合映射 $(g \circ f)$ 可能没有定义. 这个困难是由有理映射不是映射造成的, 显然复合映射定义在 $dom\ f \cap f^{-1}(dom\ g)$; 可是这很可能是空集 (见练习 4.10)

在代数表示上, 相同的问题也会发生：假如 f 是由 $f_1 \cdots, f_m \in k(V)$ 给出, 那么

$$f : V \to W \subset A^m P \mapsto f_1(P) \cdots, f_m(P)$$

对 $P \in \cap dom\ f_i$; 任意的 $g \in k[W]$ 是 $g = G\ mod\ I(W)$ 的形式, 对一些 $G \in k[Y_1 \cdots, Y_m]$ 且 $g \circ f = G(f_1 \cdots, f_m)$ 在 k(V) 上是定义良好的. 所以想 (4.4) 一样, 有一个 k-代数同态

$$f^* : k[W] \to k(V)$$

对应 f. 可是, 如果 $h \in k[W]$ 是 f^* 的 kernel, $f^*(g/h)$ 可能没意义, 所以 f^* 不能延拓到域同态 $k(W) \to k(V)$

定义 称 $f : V \to W$ 是 dominant 如果 f(dom f) 在 W 中在 Zariski 拓扑下是稠密的.

几何上, 这意味着对任意的有理映射 $g : W \to U, f^{-1}(dom\ g) \subset dom\ f$ 是稠密的开集, 所以 $g \circ f$ 定义在 V 上的稠密的开集上, 所以是部分定义的映射 $V \to U$.

代数上,

$$\text{f 是 dominant } \iff f^* k[W] \to k(V) \text{ 是单射}$$

对给定的 $g \in k[W]$,

$$g \in ker f^* \iff f(dom f) \subset V(g)$$

即 f^* 不是单射当且仅当 f(dom f) 是 W 的真子集.

显然, 有理映射 f 和 g 的复合映射 $g \circ f$ 中 f 是 dominant,$g \circ f$ 是有理映射, 由 $f^*(g_i)$ 组成. 注意到 $g \circ f$ 的定义域包含 $f^{-1}(dom\ g) \cap dom f$, 但可能会更大 (见习题 4.6)

4.11 定理

(I) 一个 dominant 的有理映射 $f : V \to W$ 定义一个域同态 $f^* : k(W) \to k(V)$.

(II) 反过来, 一个 k-同态 $\Phi : k(W) \to k(V)$ 来自一个唯一定义的有理映射 $f : V \to W$.

(III) 如果 f 和 g 是 dominant 的, 则 $(g \circ f)^* = f^* \circ g^*$

证明仅仅需要 (4.4) 做微小的变动.

4.12 来自仿射簇开集的态射

V,W 是仿射簇,$U \subset V$ 是开集.

定义 态射 $f : V \to W$ 是有理映射 $f : V \to W$ 满足 $U \subset dom f$, 所以 f 在每一点 $P \in U$ 是正则的.

如果 $U_1 \subset V, U_2 \subset W$ 是开集那么一个态射 $f : U_1 \to U_2$ 就是一个态射 $f : U_1 \to W$, 满足 $f(U_1) \subset U_2$. 同构是指一个态射两边都有逆态射.

如果 V,W 是仿射簇, 那么由同构定理 (4.8II)

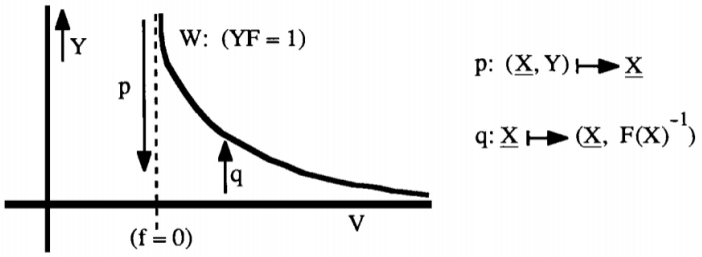
$$\{\text{ 态射 } f: V \to W\} = \{\text{ 多项式映射 } f: V \to W\}$$

例子 (2.1) 中的三次曲线参数化 $A^1 \to C : (Y^2 = X^3)$ 导出同态 $A^1\backslash\{0\} \backsimeq C\backslash\{0,0\}$, 细节见练习 4.5.

4.13 标准的开集

定理 V_f 是到仿射簇的同构, 且 $k[V_f] = k[V][f^{-1}]$.

证明想法是考虑函数 f^{-1} 的图像；使用 (3.10) 中 NSS$(b) \Rightarrow (c)$ 证明中相似的方法.



$J = I(V) \subset k[X_1, X_2 \cdots, X_n]$, 选择 $F \in k[X_1, X_2 \cdots, X_n]$ 使 $f = F \ mod \ I(V)$. 现在定义 $I = (J, YF - 1) \subset k[X_1, X_2 \cdots, X_n, Y]$, 令 $V(I) = W \subset A^{n+1}$. 很容易检验图中的映射是 V_f 和 W 之间的可逆态射, 关于坐标环的说明在 (4.8,III).

标准开集 V_f 是很重要的, 因为它形成了 V 的 Zariski 拓扑的一组基: 每一个开集 $U \subset V$ 都是一些 V_f 的并集 (因为每一个闭集的形式都是 $V(I) = \cap_{f \in I} V(f)$). 因此结果就证明了每一个开集 $U \subset V$ 都是仿射簇开集 V_f 的并集.

Chapter 5

射影几何和双有理几何

本章节的第一部分旨在概括第三章和第四章关于射影簇的内容. 剩下的部分主要关于双有理几何, 其中用到了第四章最后部分的函数域 $k(V)$, 这一部分在射影或者仿射情景下也是适合的.

5.0 为什么射影簇是簇

三次曲线

$$C : \left(Y^2Z = X^3 + aXZ^2 + bZ^3\right) \subset \mathbb{P}^2$$

是两个仿射曲线的联合:

$$C_0 : \left(y^2 = x^3 + ax + b\right) \subset \mathbb{A}^2 \quad C\text{中取}(Z = 1)\text{截面}\big)$$

和

$$C_1 : \left(z_1 = x_1^3 + axz_1 2 + bz_1^3\right) \subset \mathbb{A}^2 C\text{中取}(Y = 1)\text{截面}\big)$$

这种联合由同构

$$C_0 \backslash (y = 0) \longrightarrow C_1 \backslash (z_1 = 0)$$

$$(x, y) \mapsto (x/y, 1/y)$$

所胶合的.

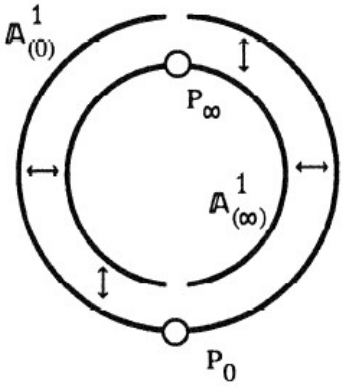
作为一个较为简单的例子, 有着齐次坐标 (X, Y) 的 $\mathbb{P}^1$ 是两个分别具有坐标 x_0, y_1 的 $\mathbb{A}^1$ 的联合, 这种联合由同构

$$\mathbb{A}^1 \backslash (x_0 = 0) \to \mathbb{A}^1 \backslash (y_1 = 0)$$

$$x_0 \quad \mapsto \quad 1/x_0$$

所胶合的.

重点是, 这种簇是严格大于仿射簇的. 事实上, 根据之后会提到的自然态射的概念, 可以看出不存在非恒定态射 $\mathbb{P}^1 \to \mathbb{A}^n$ 或 $C \to \mathbb{A}^n$ 对于任意的 n (可见习题 *5.1* 和习题 *5.12*, 在 (8.10) 中也有讨论).



一个简单的图例, 其中'↔' 代表同构

解决该问题的一种方法是采用适当的模来胶合, 而将“抽象簇”V 的概念定义为仿射簇的并集 $V = \ cup V_i$. 类似于拓扑中流形的定义, 这是一个有吸引力的想法, 但是它带来了更多的技术难题。使用射影簇可以通过在现成的环绕空间 P^n 中工作来避免这些问题, 因此（除了对齐次多项式有所了解之外）, 它们比仿射簇更难研究。实际上, 尽管在初级阶段可能还不清楚, 但是射影簇在相当可观的范围内为研究簇提供了自然的框架 (在 (8.11) 中有从更高层次的简单论述)。

5.1 分次环和齐次理想

定义 一个多项式 $f \in k[X_0 \dots X_n]$ 是 d 次齐次的, 如果

$$f = \sum a_{i_0} \cdot i_n X_0^{i_0} \dots X_n^{i_n} 其中 a_{i_0} \dots i_n \neq 0 当且仅当 i_0 + \dots i_n = d$$

对于任意 $f \in k[X_0 \dots X_n]$ 存在一个唯一的表达 $f = f_0 + f_1 + \dots f_N$ 其中 f_d 是具有 d 次齐次的多项式, 而 $d = 0, 1, \dots N$.

命题 如果 f 是 d 次齐次的, 则

$$f(\lambda X_0, \dots \lambda X_n) = \lambda d f(X_0, \dots X_n) \quad \text{for all} \quad \lambda \in k$$

如果 k 是一个无限域, 则反之亦成立.

证明

定义 一个理想 $I \subset k[X_0, \dots X_n]$ 是齐次的, 如果对于所有 $f \in I$, 在 f 的齐次分解 $f = f_0 + f_1 + \dots f_N$ 中, 对于所有 i 有 $f_i \in I$.

这等价于 I 是由 (有限个) 齐次多项式生成的.

5.2 齐次的 $V - I$ 对应

取 $\mathbb{P}_k^n$ 是一个在域 k 上的 $n-$ 维射影空间, 其中有齐次坐标 $X_0..X_n$. 则 $f \in k[X_0, \dots X_n]$ 不是一个在 $\mathbb{P}^n k$ 上的函数: 由定义,$\mathbb{P}_k^n = k^{n+1} \backslash \{0\} / \sim$, 其中 $\sim$ 是一个等价关系, 这个等价关系是 $(X_0, \dots X_n) \sim (\lambda X_0, \dots \lambda X_n)$ 其中 $\lambda \in k \backslash \{0\}$; 而 f 是一个在 k^{n+1} 上的函数. 但是, 对于 $P \in \mathbb{P}^n$, 如果 f 是齐次的, 那么条件 $f(P) = 0$ 就是良定义的: 假设 $P = (X_0 : .X_n)$, 则 $(X_0, \dots X_n)$

是 P 在 $k^{n+1}\backslash\{0\}$ 上的等价类的代表元. 因为 $f(\lambda\underline{X})=\lambda^d f(\underline{X})$, 如果 $f(X_0,\dots X_n)=0$ 那么就有 $f(\lambda X_0,\dots \lambda X_n)=0$, 因此条件 $f(P)=0$ 是独立于代表元的选取的. 出于这种想法像以前一样定义对应 V,I

$$\left\{\text{齐次理想}J\subset k[X_0,\dots X_n]\right\}\quad\overset{V,I}{\longleftrightarrow}\left\{\text{子集}X\in\mathbb{P}_k\right\}$$

其中

$$V(J)=\left\{P\in\mathbb{P}^n k|f(P)=0\forall\text{ 齐次}f\in J\right\}$$

$$I(X)=\left\{f\in k[X_0,\dots X_n]\,|\,\text{对于所有}P\in X\text{有}f(P)=0\right\}$$

作为一个练习, 想一想为什么 $I(X)$ 是一个齐次理想. 对应 V 和 I 满足仿射条件下的 V,I 的一样形式的属性 (例如 $V(J_1+J_2)=V(J_1)\cap V(J_2)$ 依然成立). $V(I)$ 的子集是 $\mathbb{P}^n_k$ 的代数子集, 类似在仿射条件下的结论, 如果在 $\mathbb{P}^n_k$ 上定义代数子集是闭集就能构造一个 Zariski 拓扑.

5.3 射影条件下的零点定理

在仿射意义的对应下，对于任意 i 理想 J 的 $I(V(J))\supset radJ$ 和对于任意代数集 X 的 $V(I(X))=X$ 是完全形式化的. 只有一点需要注意: 平凡的理想 $(1)=k[X_0\dots X_n]$(即整个环)在对应下定义了 k^{n+1} 的空集, 因此在 $\mathbb{P}^n_k$ 中同样有类似的结论; 但是, 理想 $(X_0\dots X_n)$ 同样在 k^{n+1} 上同样对应到 $\{0\}$, 即在 $\mathbb{P}^n_k$ 上同样对应空集. 理想 $(X_0\dots X_n)$ 是定理中几个论述的例外, 传统上被称为' 无关理想'.

定理 假设 k 是一个代数闭域, 则

(i) $V(J)=\varnothing\Longleftrightarrow \operatorname{rad}J\supset(X_0,\dots X_n)$

(ii) 若 $V(J)\neq\varnothing$ 则 I (V (J))= rad J

推论 I 和 V 确定可逆的双射

$$\left\{\begin{array}{c}\text{齐次根理想}J\subset k[x_0,\cdots x_n]\\ \text{其中}J\neq k[x_0,\dots x_n]\end{array}\right\}\longleftrightarrow\left\{\begin{array}{c}\text{代数子集}\\ X\subset P^n\end{array}\right\}$$

$$\cup\qquad\qquad\qquad\cup$$

$$\left\{\begin{array}{c}\text{齐次素理想}J\subset k[x_0,\cdots x_n]\\ \text{其中}J\neq k[x_0,\dots x_n]\end{array}\right\}\longleftrightarrow\left\{\begin{array}{c}\text{不可约代数子集}\\ X\subset P^n\end{array}\right\}$$

Proof. Let $\pi: A^{n+1}\backslash\{0\}\to P$ the map defining P^n. For a homogeneous ideal $J\subset k[X_0,X_n]$, write (in temporary notation) $V^a(J)\subset A^{n+1}$ for the affine algebraic set defined by J. Then since J is homogeneous, $V^a(J)$ has the property

$$(\alpha_0,\dots\alpha_n)\in v^a(J)\Longleftrightarrow(\lambda\alpha_0,\dots\alpha_n)\in v^{a(J)}$$

and $V(J)=V^{a(J)}\backslash\{0\}/\sim\subset P^n$. Hence

$$V(J)=\emptyset\Longleftrightarrow V^{a(J)}\subset\{0\}\Longleftrightarrow\operatorname{rad}J\supset(X_0\dots X_R)$$

where the last implication uses the affine Nullstellensatz. Also, if $V(J) \neq \varnothing$ then

$$f \in I(V(J)) \Longleftrightarrow f \in I\left(V^a(J)\right) \Longleftrightarrow f \in radJ, \quad Q.E.D.$$

The affine subset $V^a(J)$ occurring above is called the affine cone over the projective algebraic subset $V(J)$ (5.4) Rational functions on V. Let $V \subset P^n k$ be an irreducible algebraic set, and $I(V) \subset k\left[X_0, \ldots X_n\right]$ its ideal; there is no direct way of defining regular functions on V in terms of polynomials: an element $F \in k\left[X_0, \ldots X_N\right]$ gives a function on the