

6.2 第 17 讲 环值点与相对微分

上一讲从椭圆积分走到椭圆曲线, 又用双数环研究了点的一阶位移. 椭圆曲线也出现在整数与有理数解的研究中. 这两条线索都与方程的取值范围有关: 在整数环或有理数域中求解, 研究的是算术问题; 在双数环中求解, 还能记录点的一阶位移. 我们将从方程在环中的解出发, 比较两个点上的函数值, 再用这些函数值之差构造相对微分.

6.2.1 从费马方程到椭圆曲线

丢番图的《算术》收录了许多求多项式方程正有理数解的问题. 其中的第二卷第 8 题要求把给定的平方数写成两个正有理数的平方和, 例如书中的 $16 = (16/5)^2 + (12/5)^2$. 1621 年, 法国数学家 Claude-Gaspard Bachet 整理出版了这部书的希腊文与拉丁文对照译注本. 费马阅读此书时, 在这一题旁写下批注: 正整数的立方不能写成两个正整数的立方之和, 四次幂不能写成两个正整数的四次幂之和, 更高次幂亦然. 他还声称已找到证明, 但页边空白太小, 写不下.

用今天的记号, 费马的断言是: 对整数 $n \geq 3$, 方程 $x^n + y^n = z^n$ 没有满足 $xyz \neq 0$ 的整数解. 这样的解称为非平凡解. 将等式除以 z^n , 便得到 $r^n + s^n = 1$ 的有理数解, 其中 $r = x/z, s = y/z$. 反过来, 清除有理数解的分母就得到整数解. 因而寻找非平凡整数解, 等价于寻找满足 $rs \neq 0$ 的有理数解.

例 6.21. 设 $x, y, z \in \mathbb{Q}$ 满足 $x^3 + y^3 = z^3$ 且 $xyz \neq 0$. 此时 $x + y \neq 0$, 令

$$X = \frac{12z}{x+y}, \quad Y = \frac{36(x-y)}{x+y}.$$

恒等式 $4(x^3 + y^3) - (x+y)^3 = 3(x+y)(x-y)^2$ 给出

$$X^3 - 432 = 432 \frac{4z^3 - (x+y)^3}{(x+y)^3} = 1296 \frac{(x-y)^2}{(x+y)^2} = Y^2.$$

所以每个这样的解都给出方程 $Y^2 = X^3 - 432$ 的有理数解. 如上一讲所见, 这类三次方程的曲线补上无穷远点后, 便得到椭圆曲线.

例 6.22. 四次费马方程 $x^4 + y^4 = w^4$ 中满足 $xyw \neq 0$ 的整数解会给出 $x^4 + y^4 = z^2$ 中满足 $xyz \neq 0$ 的整数解, 只需令 $z = w^2$. 对后一个方程, 令

$$u = \frac{y^2}{x^2}, \quad v = \frac{yz}{x^3}.$$

直接计算得到 $v^2 = y^2(x^4 + y^4)/x^6 = u + u^3$. 因此, 所得的有理数 u, v 满足椭圆曲线方程 $v^2 = u^3 + u$, 其中 u 还是有理数的平方.

费马用无限递降法证明, 整数直角三角形的面积不可能是平方数. 这个结论也排除了四次费马方程的非平凡解.¹ 递降法从假想的整数解构造出更小的同类解, 利用正整数不能无限严格递减得到矛盾. 1670 年, 费马的儿子 Samuel 将父亲对丢番图的批注编入新版《算术》, 刊出了他对所有指数 $n \geq 3$ 的断言及上述递降证明.

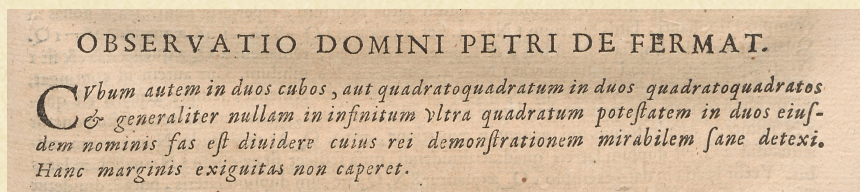


图 6.8: 左: 费马的 17 世纪雕版肖像. 右: 1670 年版丢番图《算术》第 61 页, 费马批注的刊印文字.²

德国数学家 Gerhard Frey 提出了费马问题与椭圆曲线的另一条联系: 由假想的解构造一条辅助曲线. 假设素数 $p \geq 5$ 的费马方程有互素的非零整数解 $a^p + b^p = c^p$, 便考虑

$$y^2 = x(x - a^p)(x + b^p).$$

右端的三个根 $0, a^p, -b^p$ 互异, 因为 $ab \neq 0$ 且 $a^p + b^p = c^p \neq 0$. 补上无穷远点后, 这就是通常所说的 Frey 曲线.

〔史略〕 一条算术路线



Andrew Wiles

谷山丰、志村五郎发展的猜想预言, 有理数域上的椭圆曲线都与一类称为模形式的解析函数对应. Frey 提出, 费马反例应能给出违反猜想的曲线. Jean-Pierre Serre 将所需的关键推断表述为精确猜想, Kenneth Ribet 于 1986 年证明了它: 从费马反例适当选取的 Frey 曲线不可能有这种对应. Andrew Wiles 则证明包括这些曲线在内的一类椭圆曲线都有这种对应, 矛盾排除了费马反例. 关键一步由他与 Richard Taylor 合作完成, 两篇论文于 1995 年发表. 2016 年, Wiles 因这项工作获阿贝尔奖.³

¹ 由非平凡解 $x^4 + y^4 = w^4$ 得整数直角三角形 $(2x^2w^2, y^4, x^4 + w^4)$, 其面积为 $(xwy^2)^2$.

² 肖像: François de Poilly 雕版, 原图. 书影: Diophantus, *Arithmeticon libri sex*, Bachet 译注, Samuel de Fermat 编, 1670, 第 61 页; 递降证明见第 338–339 页. ETH-Bibliothek Zürich, Rar 3625, 数字原件. 1621 年版书目.

³ A. Wiles, *Ann. of Math.* 141 (1995), 443–551, 引言及定理 0.4 (有理数域上半稳定椭圆曲线的模性); K. Ribet, *Invent. Math.* 100 (1990), 431–476, 定理 1.1、推论 1.2; R. Taylor 与 A. Wiles, *Ann. of Math.* 141 (1995), 553–572. 2016 年阿贝尔奖官方说明. 照片: IAS, 2005; copyright C. J. Mozzochi, Princeton N.J; Courtesy of the Simons Foundation, 按原图许可裁切.

6.2.2 椭圆曲线上的有理点怎样相加

设 $a, b \in \mathbb{Q}$, 且多项式 $x^3 + ax + b$ 没有重根, 即 $4a^3 + 27b^2 \neq 0$. 方程 $y^2 = x^3 + ax + b$ 的曲线补上无穷远点 O 后得到椭圆曲线 E . 坐标为有理数的解称为曲线的有理点, 而 O 也是有理点. 因而

$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + ax + b\} \sqcup \{O\}.$$

这些点可以相加. 先取两个横坐标不同的点 P, Q , 过它们作直线, 与曲线交于第三点 S (允许与 P 或 Q 重合); 把 S 关于横轴对称, 所得的点就定义为 $P + Q$. 若 $P = Q$ 且纵坐标非零, 则把连线换成曲线在 P 处的切线, 切点算作两次交点, 余下的第三交点仍允许是 P . 这称为弦切法.

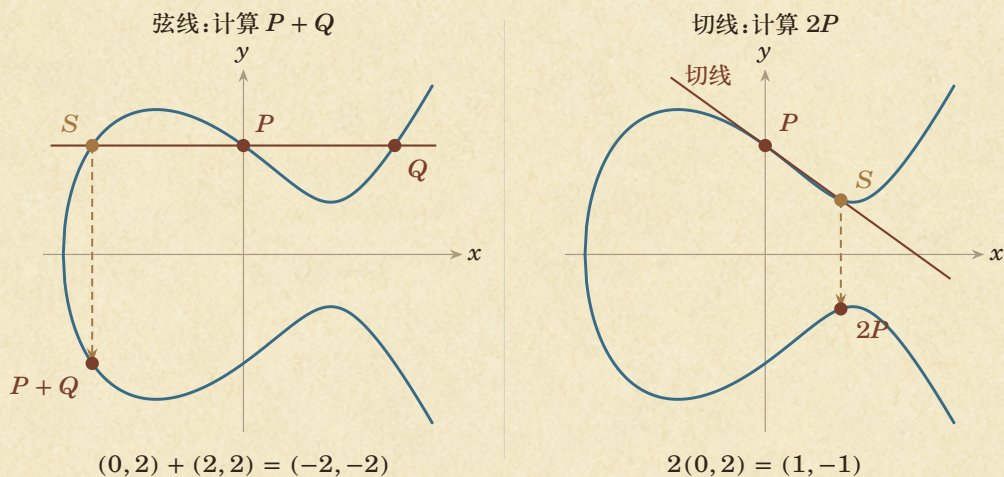


图 6.9: 曲线 $y^2 = x^3 - 4x + 4$ 上的弦切法. 弦线或切线确定第三交点 S , 金色虚线箭头把它关于横轴对称, 得到所求的和.

这一作图保持有理坐标. 例如设 $P = (x_1, y_1), Q = (x_2, y_2)$ 且 $x_1 \neq x_2$, 连线的斜率为 $m = (y_2 - y_1)/(x_2 - x_1)$. 将直线方程代入三次方程, 由三根之和得第三交点的横坐标为 $m^2 - x_1 - x_2$, 仍是有理数. 对称后的纵坐标也由有理数的加减乘除得到. 两点重合且 $y_1 \neq 0$ 时, 切线斜率为 $(3x_1^2 + a)/(2y_1)$, 同样是有理数.

竖直线经过 $(x, y), (x, -y)$ 和无穷远点 O , 相应地规定 $(x, y) + (x, -y) = O$; 当 $y = 0$ 时, 这表示该点与自身相加得到 O . 再规定 $P + O = O + P = P$. 这样, 关于横轴对称就是取负元, 弦切法的规则便写成 $P + Q + S = O$: 共线的三个交点之和为零. 弦切法连同这些规则使 $E(\mathbb{Q})$ 成为阿贝尔群; 结合律的证明需要核对三点相加的两种顺序, 详见脚注中的参考文献.⁴

⁴A. V. Sutherland, *18.783 Elliptic Curves, Lecture 2*, 2025, §2.1–2.2, 第 1–4 页; §2.2 及配套计算验证包括特殊情形在内的结合律.

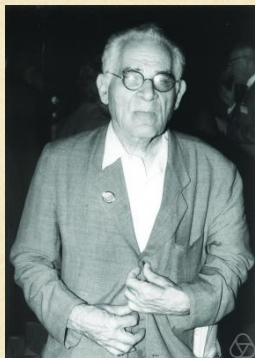
有了加法,就能问:是否只需有限多个点,反复相加、取负,便能得到所有有理点?其中,满足 $nP = O$ (某个正整数 n) 的点称为有限阶点,它们组成的子群记为 $E(\mathbb{Q})_{\text{tors}}$,称为挠子群.

定理 6.23 (Mordell–Weil). 有理数域上椭圆曲线 E 的有理点群 $E(\mathbb{Q})$ 是有限生成阿贝尔群. 因而存在整数 $r \geq 0$, 使

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}},$$

且挠子群 $E(\mathbb{Q})_{\text{tors}}$ 是有限群.

整数 r 称为 $E(\mathbb{Q})$ 的秩; $r = 0$ 时有理点只有有限个, $r > 0$ 时则有无穷多个. Louis Mordell 于 1922 年证明了有理数域上的结论, André Weil 在 1928 年博士论文中将它推广到有理数域的任意有限扩域.⁵



Mordell



Weil⁶

6.2.3 方程在环中的解

有理数只是方程的一种取值范围. 同一组整系数方程还可以在 $\mathbb{Z}$ 、 $\mathbb{R}$ 、 $\mathbb{C}$ 或有限域中求解. 以平面抛物线 $t = y^2$ 为例, 横坐标记为 t . 对环 R , 记其解集为 $P(R) = \{(r, s) \in R^2 : r = s^2\}$. 若 $\varphi : R \rightarrow R'$ 为环同态, 则 $r = s^2$ 蕴含 $\varphi(r) = \varphi(s)^2$, 所以逐坐标应用 φ 给出映射 $P(R) \rightarrow P(R')$. 恒等同态不改变解, 两个环同态的复合则对应解集映射的复合.

对于系数属于环 A 的方程, 取值环 R 配有结构同态 $A \rightarrow R$, 即 R 是 A -代数. 在这样的代数之间, A -代数同态保持来自 A 的系数. 方程的解可以用这类同态来描述.

⁵L. J. Mordell, *On the Rational Solutions of the Indeterminate Equations of the Third and Fourth Degrees*, *Proc. Cambridge Philos. Soc.* 21 (1922), 179–192, 尤其第 180, 191 页. A. Weil, *L'arithmétique sur les courbes algébriques*, 1928 年, 引言及 §13, §20; 期刊版发表于 *Acta Math.* 52 (1929), 281–315.

⁶两图均为 Konrad Jacobs 摄, 版权 MFO, CC BY-SA 2.0 DE. 左: Mordell, Nice, 1970, 原图. 右: Weil, Oberwolfach, 1968, 馆藏 8654 号合照的已发表裁切版.

命题 6.24. 设 A 为环, $f_1, \dots, f_s \in A[t_1, \dots, t_n]$, 令 $B = A[t_1, \dots, t_n]/(f_1, \dots, f_s)$. 对每个 A -代数 R , 有双射

$$\begin{aligned} \mathrm{Hom}_{A\text{-Alg}}(B, R) &\simeq \{r \in R^n : f_1(r) = \dots = f_s(r) = 0\}, \\ u &\longmapsto (u(\bar{t}_1), \dots, u(\bar{t}_n)), \end{aligned}$$

其中 $r = (r_1, \dots, r_n)$, $\bar{t}_i$ 是 t_i 在 B 中的像, 左端表示全体 A -代数同态.

证明. 一个 A -代数同态 $A[t_1, \dots, t_n] \rightarrow R$ 由各 t_i 的像 r_i 唯一决定. 它经过商环 B 分解, 当且仅当每个 f_j 都映到零, 也就是 $f_j(r_1, \dots, r_n) = 0$. 两种构造互逆. $\square$

因此, 指定方程在 R 中的一组解, 等价于指定从其坐标环 B 到 R 的 A -代数同态: 解的各坐标就是 $\bar{t}_i$ 的像. 这启发我们对任意 A -代数作如下定义.

定义 6.25. 设 B 为 A -代数, $X = \mathrm{Spec} B$. 对 A -代数 R , 称 A -代数同态 $B \rightarrow R$ 为 X 的 R -值点, 并记 $X(R) = \mathrm{Hom}_{A\text{-Alg}}(B, R)$. 若 $\varphi : R \rightarrow R'$ 为 A -代数同态, 定义

$$X(\varphi) : X(R) \rightarrow X(R'), \quad u \longmapsto \varphi \circ u.$$

这样得到的函子 $X(-) : A\text{-Alg} \rightarrow \mathbf{Set}$ 称为 X 的点函子 (*functor of points*).

这里 $A\text{-Alg}$ 是 A -代数及其同态组成的范畴, $\mathbf{Set}$ 是集合范畴. 从几何上说, R -值点也就是 $\mathrm{Spec} A$ 上的态射 $\mathrm{Spec} R \rightarrow X$. 对整系数或有理系数方程, 取 $R = \mathbb{Q}$, 便恢复了方程有理点的含义. 例如三次方程 $y^2 = x^3 + ax + b$ 的有理数解, 对应的是 $E(\mathbb{Q})$ 中除去 O 的点; O 不在这张平面坐标图中.

例 6.26. 对 $P = \mathrm{Spec}(\mathbb{Z}[t, y]/(t - y^2))$, 定义给出的 $P(R)$ 正是前面抛物线的解集. 在 $\mathbb{R}$ 中, 实点组成抛物线; 在 $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ 中, 点集是

$$P(\mathbb{F}_5) = \{(0, 0), (1, 1), (4, 2), (4, 3), (1, 4)\}.$$

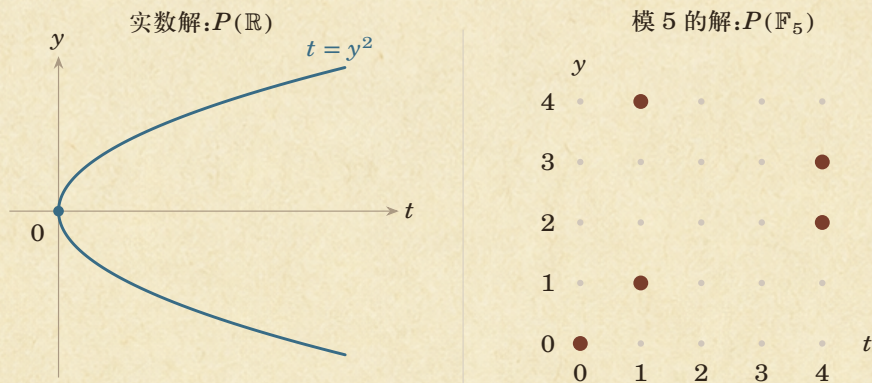


图 6.10: 方程 $t = y^2$ 在 $\mathbb{R}$ 与 $\mathbb{F}_5$ 中的解. 左图是实抛物线; 右图的 25 个格点表示 $\mathbb{F}_5^2$, 其中五个实心点满足方程.

〔史略〕 Grothendieck 与点函子



Alexander
Grothendieck

Grothendieck 系统地用点函子研究几何对象: 同时考察每个环中的点, 以及环同态所诱导的点集映射. 在 1960 年 2 月的 Bourbaki 报告中, 他把“将对象送到它的点函子”这一对应记为 h , 并回顾其范畴论性质:

Ce foncteur h est pleinement fidèle.

即“这个函子 h 是满忠实的”. 具体说, $\text{Spec} A$ 上的态射 $X \rightarrow X'$ 与点函子之间的自然变换 $X(-) \rightarrow X'(-)$ 一一对应. 所有环中的点集, 连同环同态诱导的映射, 足以在同构意义下确定几何对象.⁷

我们为仿射概形验证这一对应. 设 B, B' 为 A -代数, $X = \text{Spec} B$, $X' = \text{Spec} B'$. 回顾第十二讲, $\text{Spec} A$ 上的态射 $X \rightarrow X'$ 由反向的 A -代数同态 $B' \rightarrow B$ 给出. 对自然变换 $\eta : X(-) \rightarrow X'(-)$, 取 $R = B$ 及点 $\text{id}_B \in X(B)$, 便得到这样的同态 $\theta = \eta_B(\text{id}_B) : B' \rightarrow B$.

自然性具体要求: 对每个 A -代数同态 $\varphi : R \rightarrow R'$ 及每个 $u \in X(R)$, 都有

$$\eta_{R'}(\varphi \circ u) = \varphi \circ \eta_R(u).$$

其中, $u : B \rightarrow R$, 两边都是从 B' 到 R' 的同态. 把这里的 R, u, φ 分别取为 B, id_B, v , 其中 $v : B \rightarrow R'$, 便得 $\eta_{R'}(v) = v \circ \theta$. 反过来, 每个 A -代数同态 $\theta : B' \rightarrow B$ 都通过此公式给出自然变换. 这就得到了 $\text{Spec} A$ 上的态射 $X \rightarrow X'$ 与自然变换的一一对应.

⁷A. Grothendieck, Bourbaki 报告 195, 1960 年 2 月, §A.1, 命题 1.1 及第 369–371 页. 这里的满忠实性是 Yoneda 引理的推论; 引理的归属见 S. Mac Lane, *The Yoneda Lemma*, *Mathematica Japonica* 47 (1998), 第 156 页. 肖像: Konrad Jacobs 摄, 1970, 版权 MFO; 原图, CC BY-SA 2.0 DE.

6.2.4 从点处导子到相对导子

为什么把点的取值范围放宽到一般环,而不只考虑域?上一讲的双数环给出了理由:它能记录点的一阶位移.例如设 k 为域, $a, v \in k$, 把抛物线坐标 y 的值取成 $a + v\epsilon \in k[\epsilon]/(\epsilon^2)$, 则 $t = y^2$ 的值为 $a^2 + 2av\epsilon$. 常数项给出点 (a^2, a) , ϵ 的系数给出切向量 $(2av, v)$. 若取值环是域,平方为零的元素只能是零,这部分信息就消失了.

更一般地,设 B 为 k -代数, $p: B \rightarrow k$ 为 k -有理点,记 $b(p) = p(b)$, $\mathfrak{m} = \ker p$. 满足常数项为 p 的 k -代数同态

$$\tilde{p}: B \rightarrow k[\epsilon]/(\epsilon^2), \quad \tilde{p}(b) = b(p) + D(b)\epsilon$$

对应于 k -线性映射 $D: B \rightarrow k$, 其乘法公式为 $D(bc) = b(p)D(c) + c(p)D(b)$. 把 k 看作通过 p 作用的 B -模, 这就是 $D(bc) = bD(c) + cD(b)$. 这些导子组成的空间记为 $\text{Der}_{k,p}(B, k)$. 命题 6.15 已证明

$$\text{Der}_{k,p}(B, k) \simeq \text{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, k).$$

此处 $\mathfrak{m}/\mathfrak{m}^2$ 的 k -向量空间结构, 来自 $B/\mathfrak{m} = k$ 对它的作用.

现在固定环同态 $\alpha: A \rightarrow B$, 它在几何上给出映射 $\text{Spec } B \rightarrow \text{Spec } A$. 要求来自 A 的函数在求导时保持不变, 就能考察投影到底空间后不动的一阶变化. 导子的值也可以是函数, 而不限于点处的数: 例如求导 $k[y] \rightarrow k[y]$ 的结果仍是多项式, 在 $y = a$ 处取值后才得到 k -值导子. 为同时处理这些情况, 我们允许导子取值于 B -模.

定义 6.27. 设 $\alpha: A \rightarrow B$ 为环同态, M 为 B -模. 加法群同态 $D: B \rightarrow M$ 称为 A -导子, 如果对所有 $b, c \in B$ 及 $a \in A$ 都有

$$D(bc) = bD(c) + cD(b), \quad D(\alpha(a)) = 0.$$

全体这样的导子记为 $\text{Der}_A(B, M)$.

第一条是莱布尼茨法则, 第二条说明哪些量被当作常数. 两条合起来给出 $D(\alpha(a)b) = \alpha(a)D(b)$, 所以 D 是 A -线性的. 一般不能把它当作 B -线性映射; 例如 $\mathbb{Q}[x]$ 上的求导满足 $D(x^2) = 2x$, 而 $xD(x) = x$.

通过 $(D_1 + D_2)(b) = D_1(b) + D_2(b)$ 与 $(cD)(b) = cD(b)$, 集合 $\text{Der}_A(B, M)$ 成为 B -模: 将定义中的等式相加或乘以 $c \in B$, 等式仍成立.

例 6.28. 设 $B = A[x]$, M 为 B -模. 任一 A -导子 $D: B \rightarrow M$ 都由 $m = D(x)$ 唯一决定. 由莱布尼茨法则归纳得 $D(x^j) = jx^{j-1}m$ ($j \geq 1$), 因此对多项式 $g \in A[x]$ 有 $D(g) = g'(x)m$, 其中 g' 为形式导数. 反过来, 对任意 $m \in M$, 这个公式都定义一个 A -导子: 形式导数保持加法, 其莱布尼茨法则可对单项式直接验证.

6.2.5 两个点、函数差与对角线

给定环同态 $\alpha: A \rightarrow B$, 记 $X = \operatorname{Spec} B, Y = \operatorname{Spec} A$. 上一节定义的 A -导子满足 $D(\alpha(a)) = 0$, 即来自底空间 Y 的函数不发生一阶变化. 为了用函数差构造 A -导子, 我们比较投影到 Y 后相同的两个点.

取环 R 及两个环同态 $u, v: B \rightarrow R$, 要求 $u \circ \alpha = v \circ \alpha$. 用这一共同合成赋予 R 以 A -代数结构, u, v 就是两个 A -代数同态. 张量积的泛性质给出唯一的 A -代数同态

$$B \otimes_A B \rightarrow R, \quad b \otimes c \mapsto u(b)v(c).$$

反过来, 给定一个 A -代数同态 $q: B \otimes_A B \rightarrow R$, 令 $u(b) = q(b \otimes 1), v(b) = q(1 \otimes b)$, 便恢复这两个点. 这就是仿射概形纤维积 $X \times_Y X = \operatorname{Spec}(B \otimes_A B)$ 的点所表达的内容.

在点对 (u, v) 上, 函数 $b \otimes 1$ 与 $1 \otimes b$ 分别取值为 $u(b)$ 与 $v(b)$. 因而函数差 $\delta(b) = 1 \otimes b - b \otimes 1$ 取值为 $v(b) - u(b)$.

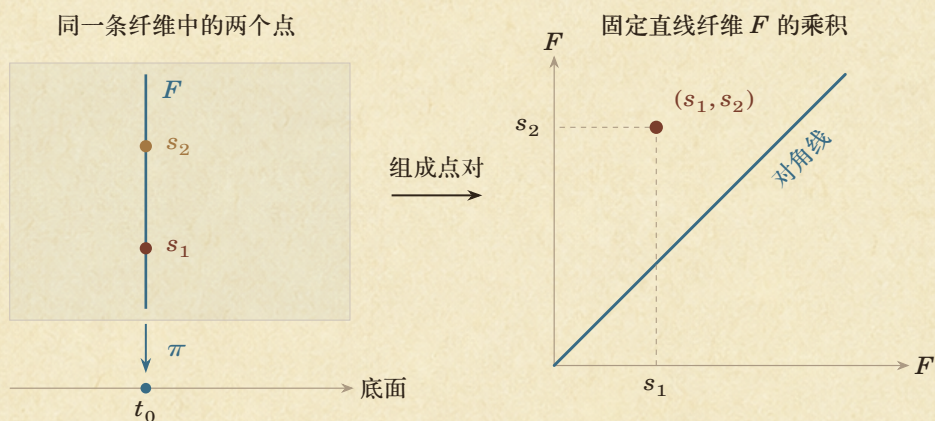


图 6.11: 左: 实平面向水平轴的投影 π, s_1, s_2 位于 t_0 上方的同一条纤维 F 中. 右: 固定这条直线纤维, 点对组成平面 $F \times F$; 对角线上的两个坐标相等.

若把两个点取成同一点, 函数 $b \otimes c$ 就取值为 $u(b)u(c) = u(bc)$. 这提示我们考虑乘法同态

$$\mu: B \otimes_A B \rightarrow B, \quad b \otimes c \mapsto bc.$$

它是满射, 因为 $\mu(b \otimes 1) = b$. 由 μ 诱导的态射 $\Delta: X \rightarrow X \times_Y X$ 在 R -值点上正是 $u \mapsto (u, u)$, 称为对角态射. 记 $I = \ker \mu$, 则 $(B \otimes_A B)/I \simeq B, I$ 就是定义这条对角线的理想.

引理 6.29. 设 $\alpha: A \rightarrow B$ 为环同态, I 为乘法同态 $\mu: B \otimes_A B \rightarrow B$ 的核. 则 I 由全部 $\delta(b) = 1 \otimes b - b \otimes 1 (b \in B)$ 生成. 更精确地, 若 $z = \sum_{j=1}^n b_j \otimes c_j \in I$, 则

$$z = \sum_{j=1}^n (b_j \otimes 1) \delta(c_j).$$

证明. 每个 $\delta(b)$ 都属于 I . 反之, $z \in I$ 意味着 $\sum_j b_j c_j = 0$, 因而

$$\sum_j (b_j \otimes 1) \delta(c_j) = \sum_j b_j \otimes c_j - \left(\sum_j b_j c_j \right) \otimes 1 = z.$$

这同时给出了生成性和所述公式. □

6.2.6 相对微分模

上一讲把点处消失的函数组成理想 $\mathfrak{m}$, 再模去 $\mathfrak{m}^2$, 留下函数的一阶部分. 现在, 函数差 $\delta(b)$ 生成对角线的理想 I ; 模去 I^2 , 便忽略两个函数差的乘积. 商 I/I^2 将记录两个点重合时, 函数差的一阶信息.

先明确这个商的标量作用. I/I^2 是 $B \otimes_A B$ -模, 而且 I 中每个元素在它上的作用都为零. 因此作用经过 $(B \otimes_A B)/I \simeq B$ 分解, 使 I/I^2 成为 B -模. 具体地, 对 $b \in B$, $z \in I$, 定义

$$b \cdot (z + I^2) = (b \otimes 1)z + I^2.$$

换用 $1 \otimes b$ 得到相同结果, 因为两者之差为 $\delta(b)z \in I^2$.

定义 6.30. 设 $\alpha : A \rightarrow B$ 为环同态, I 为乘法同态 $B \otimes_A B \rightarrow B$ 的核. 称 B -模 $\Omega_{B/A}^1 = I/I^2$ 为 B 在 A 上的 Kähler 微分模, 并定义映射

$$d_{B/A} : B \rightarrow \Omega_{B/A}^1, \quad b \mapsto db = (1 \otimes b - b \otimes 1) + I^2.$$

底环和代数明确时, 把 $d_{B/A}$ 简记为 d .

命题 6.31. 对环同态 $\alpha : A \rightarrow B$, 映射 $d : B \rightarrow \Omega_{B/A}^1$ 是 A -导子, 且 $\Omega_{B/A}^1$ 由所有 db ($b \in B$) 作为 B -模生成.

证明. 映射 d 保持加法. 在对 A 的张量积中, 标量可以从一边移到另一边, 因此 $1 \otimes \alpha(a) = \alpha(a) \otimes 1$, 所以 $d\alpha(a) = 0$. 为验证乘法公式, 在 $B \otimes_A B$ 中展开得

$$\delta(bc) = (b \otimes 1)\delta(c) + (c \otimes 1)\delta(b) + \delta(b)\delta(c).$$

最后一项属于 I^2 , 故在商模中得到 $d(bc) = bdc + cdb$. 引理 6.29 的生成公式取模 I^2 后, 说明各 db 生成整个微分模. □

例 6.32. 取 $B = A[x]$, 记 $x_1 = x \otimes 1$, $x_2 = 1 \otimes x$, 则 $B \otimes_A B \simeq A[x_1, x_2]$. 乘法同态把 x_1, x_2 都送到 x , 因而 $I = (x_2 - x_1)$. 令 $h = x_2 - x_1$, 在商环 $(B \otimes_A B)/I^2 \simeq A[x_1, h]/(h^2)$ 中, 对 $g \in A[x]$, 多项式展开给出

$$g(x_2) - g(x_1) = g(x_1 + h) - g(x_1) = g'(x_1)h.$$

这正是形式微分 $dg = g'(x) dx$, 其中 dx 对应 h 在 I/I^2 中的像. 每个 I/I^2 中的元素都唯一写成 $g(x_1)h + I^2$, 故 $\Omega_{A[x]/A}^1$ 是以 dx 为基的自由 $A[x]$ -模.

定理 6.33. 设 $\alpha: A \rightarrow B$ 为环同态, M 为 B -模. 复合 $d: B \rightarrow \Omega_{B/A}^1$ 给出 B -线性同构

$$\mathrm{Hom}_B(\Omega_{B/A}^1, M) \simeq \mathrm{Der}_A(B, M), \quad \ell \mapsto \ell \circ d.$$

即每个 A -导子 $D: B \rightarrow M$ 都唯一写成 $D = \tilde{D} \circ d$, 其中 $\tilde{D}$ 为 B -线性映射.

证明. 因 d 是导子, 任一 B -线性映射 ℓ 与它复合后仍满足导子的两条条件. 这给出了陈述中的映射. 下面证明它为双射.

给定 A -导子 $D: B \rightarrow M$, 考虑 $(b, c) \mapsto bD(c)$. 它对两个变量都可加, 并且对 $a \in A$ 有

$$(\alpha(a)b)D(c) = b\alpha(a)D(c) = bD(\alpha(a)c).$$

由张量积的泛性质, 它诱导加法群同态 $F: B \otimes_A B \rightarrow M$, 满足 $F(b \otimes c) = bD(c)$, 并且 $F((b \otimes 1)z) = bF(z)$. 因 $D(1) = 0$, 有 $F(\delta(c)) = D(c)$. 命题 6.31 中的乘积恒等式给出

$$F(\delta(b)\delta(c)) = D(bc) - bD(c) - cD(b) = 0.$$

引理 6.29 把 I 中每个元素写成 $\sum_j (b_j \otimes 1)\delta(c_j)$; 将两式相乘, 可知 I^2 中每个元素都是 $(b \otimes 1)\delta(c)\delta(c')$ 的有限和. 因而 F 消去 I^2 .

把 F 限制到 I 并取商, 得到 B -线性映射 $\tilde{D}: I/I^2 \rightarrow M$, 且

$$\tilde{D}(db) = F(1 \otimes b - b \otimes 1) = D(b) - bD(1) = D(b).$$

这证明了存在性. 由于所有 db 生成 $\Omega_{B/A}^1$, 等式 $\tilde{D}(db) = D(b)$ 又唯一决定 $\tilde{D}$. 最后, 复合 d 保持加法与 B -数乘, 故这个双射是 B -线性的. $\square$

这个泛性质也唯一确定了微分模: 若 N 为 B -模, $d': B \rightarrow N$ 为 A -导子, 且 (N, d') 对所有 B -模都有相同的分解性质, 则分别应用于 d 和 d' , 得到互逆的 B -线性同构, 且同构把 db 送到 $d'b$.

〔史略〕 代数中的微分

前面的泛性质说明,微分模把 A -导子表示为 B -线性映射. 微分模的代数定义可追溯到 Erich Kähler 的 1953 年论文《代数与微分学》. Pierre Cartier 在 1956 年的讲义中用导子的泛性质刻画微分模,并讲解了 I/I^2 的构造. Grothendieck 则用对角线及其一阶邻域研究解析空间和概形的相对微分.^a 把对角线的定义理想 I 换成 I^2 ,得到其一阶邻域

$$\mathrm{Spec}((B \otimes_A B)/I^2).$$

素理想包含 I^2 当且仅当包含 I ,所以这一邻域与对角线的底层拓扑空间相同;它的函数环中还保留了平方零理想 I/I^2 .

^aKähler 工作的历史介绍据 L. Illusie, *Grothendieck and differential calculus*, *C. R. Math.* 363 (2025), 第 830 页脚注 2 及文献 [37];该文将定义追溯至 Kähler 的 *Algebra und Differentialrechnung* (1953), 58–163. Cartier 原文见 *Dérivations dans les corps*, *Séminaire Henri Cartan* 8 (1955–1956), 报告 13, 1956 年 2 月 13, 20 日, 第 13-01–13-02 页.



Erich Kähler

Pierre Cartier⁸

6.2.7 抛物线的相对微分

回到抛物线 $t = y^2$ 向 t 轴的投影. 沿这一投影求相对微分时,把底坐标 t 当作常数;由 $t = y^2$ 得到 $d(y^2) = 2y dy = 0$. 下面用泛性质计算相应的微分模.

例 6.34. 设 k 为域, $A = k[t]$, $B = k[y]$, 以 k -代数同态 $\alpha : A \rightarrow B, t \mapsto y^2$ 赋予 B 以 A -代数结构. 则

$$\Omega_{B/A}^1 \simeq (B/(2y)) dy.$$

若 $\mathrm{char} k \neq 2$,这等于 $(B/(y)) dy$;若 $\mathrm{char} k = 2$,则等于 $B dy$.

给定 B -模 M , 一个 k -导子 $D : B \rightarrow M$ 由 $m = D(y)$ 唯一决定, 公式为 $D(g) = g'(y)m$. 它是 A -导子, 当且仅当它消去 y^2 : 必要性来自 $y^2 = \alpha(t)$; 充分性则因 A 的像

⁸左: Konrad Jacobs 摄, Hamburg, 1990, 版权 MFO, Commons 原图, CC BY-SA 2.0 DE. 右: Andrej Bauer 图库提供, Firenze, 2003 年 11 月, 图库原图, CC BY-SA 2.5 SI; 图示为原照片局部, 保留同一许可.

由 k 和 y^2 生成. 这一条件恰为 $2ym = 0$.

另一方面, 从 $(B/(2y))dy$ 到 M 的 B -线性映射, 也由满足 $2ym = 0$ 的元素 m 唯一决定, 只需令 $dy \mapsto m$. 因而这个商模及 $g \mapsto g'(y)dy$ 满足微分模的泛性质, 得出所述同构. 这也说明 $2ydy = 0$ 之外没有额外的关系.

也可用对角线核对这个关系. 在 $B \otimes_A B$ 中记 $y_1 = y \otimes 1, y_2 = 1 \otimes y$, 则 $y_2^2 = y_1^2$. 令 $h = y_2 - y_1$, 便得 $2y_1h + h^2 = 0$. 模去 I^2 后, h^2 消失, 留下的 $2y_1h = 0$ 正是 $2ydy = 0$.

假设 $\text{char } k \neq 2$, 并取 $a \in k$. 沿取值同态 $\text{ev}_a : B \rightarrow k, g \mapsto g(a)$ 扩张标量, 得到向量空间 $\Omega_{B/A}^1 \otimes_{B, \text{ev}_a} k$, 称为微分模在点 $y = a$ 处的纤维. 因而

$$\Omega_{B/A}^1 \otimes_{B, \text{ev}_a} k \simeq \begin{cases} 0, & a \neq 0, \\ k(dy \otimes 1), & a = 0. \end{cases}$$

点 $y = a$ 处的切向量由 $v = D(y) \in k$ 决定, 它在底空间坐标上的变化为 $D(\alpha(t)) = D(y^2) = 2av$. 满足 $2av = 0$ 的切向量投影后为零, 称为这一投影的相对切向量. 当 $a \neq 0$ 时只有零向量; 在原点则 v 可以任取. 以 ev_a 赋予 k 以 B -模结构, 这些相对切向量组成 $\text{Der}_A(B, k)$. 由定理 6.33 与张量-Hom 伴随,

$$\text{Der}_A(B, k) \simeq \text{Hom}_B(\Omega_{B/A}^1, k) \simeq \text{Hom}_k(\Omega_{B/A}^1 \otimes_{B, \text{ev}_a} k, k),$$

所以相对切向量空间正是微分模纤维的 k -线性对偶.

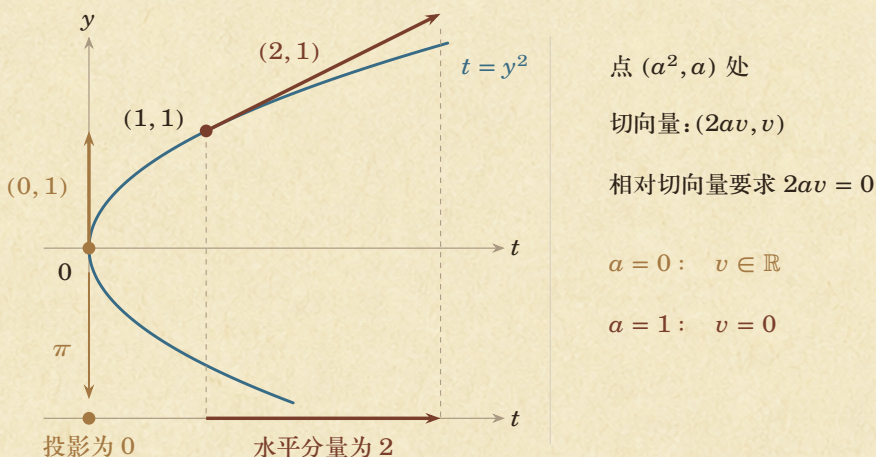


图 6.12: 实抛物线 $(t, y) = (y^2, y)$ 的切向量及其投影. 原点处的竖直切向量投影为零; 在 $y = 1$ 处, 切向量 $(2, 1)$ 投影为非零的水平向量.

在 $\text{char } k = 2$ 时, $2av$ 恒为零, 所以每个 k -有理点都允许非零的相对切向量. 这与实数域上的情形不同, 原因在于特征 2 中形式导数 $(y^2)'$ 恒为零.

6.2.8 微分模在点处的取值

刚才固定投影的底空间坐标,考察留在同一条纤维中的一阶变化. 现在只固定域 k 中的常数,研究空间本身的一阶变化. 微分模在点 $p: B \rightarrow k$ 处的纤维,将恢复上一讲的余切空间.

命题 6.35. 设 k 为域, B 为 k -代数. 对任意 k -有理点 $p: B \rightarrow k$, 记 $\mathfrak{m} = \ker p$, 则下列映射为 k -线性同构:

$$\begin{aligned} \Omega_{B/k}^1 \otimes_{B,p} k &\simeq \mathfrak{m}/\mathfrak{m}^2, \\ db \otimes \lambda &\mapsto \lambda(b - b(p) + \mathfrak{m}^2) \quad (b \in B, \lambda \in k). \end{aligned}$$

证明. 在 B -模 $\mathfrak{m}/\mathfrak{m}^2$ 上, B 通过 p 作用. 定义 $\partial: B \rightarrow \mathfrak{m}/\mathfrak{m}^2$, 令 $\partial(b) = b - b(p) + \mathfrak{m}^2$. 命题 6.15 的证明已经计算了乘积模 $\mathfrak{m}^2$ 的一次项, 由此可知 ∂ 是 k -导子. 由泛性质, ∂ 诱导 B -线性映射 $\Omega_{B/k}^1 \rightarrow \mathfrak{m}/\mathfrak{m}^2$. 因目标的 B -作用经过 p , 它诱导所述 k -线性映射.

反过来, 对 $u \in \mathfrak{m}$, 令 $u + \mathfrak{m}^2 \mapsto du \otimes 1$. 若 $u = vw$, 其中 $v, w \in \mathfrak{m}$, 则

$$d(vw) \otimes 1 = dw \otimes v(p) + dv \otimes w(p) = 0.$$

因此这个加法映射消去 $\mathfrak{m}^2$, 给出良定义的 k -线性映射 $\mathfrak{m}/\mathfrak{m}^2 \rightarrow \Omega_{B/k}^1 \otimes_{B,p} k$. 两个复合在生成元 $u + \mathfrak{m}^2$ 和 $db \otimes 1$ 上分别为恒等映射, 故互为逆. $\square$

于是, $\Omega_{B/k}^1$ 在点 p 处的纤维就是余切空间, 其 k -线性对偶就是切空间.

再看抛物线投影在 $t = a^2$ 处的纤维, 其方程为 $y^2 = a^2$, 坐标环为 $k[y]/(y^2 - a^2)$. 点 $y = a$ 处的 A -导子消去 $y^2 - a^2$; 由莱布尼茨法则, 它也消去这个元素生成的理想, 因而唯一经过该商环分解. 反过来, 商环上的 k -导子给出原来的 A -导子. 所以, 上一节的相对切向量组成的空间, 恰是这条纤维在 $y = a$ 处的切空间, 亦即其余切空间的对偶.

6.2.9 从微分模到余切层

对任意环同态 $A \rightarrow B$, 微分模 $\Omega_{B/A}^1$ 都有定义. 因此, 同一构造既能用于实数、复数上的代数曲线, 也能用于有限域上的方程、含幂零元的环以及以整数环为底环的方程. 从仿射概形推广到一般概形的关键, 是让局部的微分模在交叠处一致.

先看局部化. 设 $A \rightarrow B$ 为环同态, $g \in B$. 在 $\Omega_{B_g/A}^1$ 中计算微分, 由 $g \cdot g^{-1} = 1$ 得 $d(g^{-1}) = -g^{-2}dg$, 所以微分在分式上的值必须满足

$$d\left(\frac{b}{g^n}\right) = \frac{db}{g^n} - \frac{nb dg}{g^{n+1}} \quad (b \in B, n \geq 0).$$

这个公式也把每个 A -导子 $D: B \rightarrow M$ 唯一延拓到 B_g , 只要 M 是 B_g -模. 为验证良定义, 将分子分母同乘 g , 由莱布尼茨法则得

$$\frac{D(bg)}{g^{n+1}} - \frac{(n+1)bgD(g)}{g^{n+2}} = \frac{D(b)}{g^n} - \frac{nbD(g)}{g^{n+1}}.$$

若两个分式相等, 按局部化中分式相等的定义, 总能各自将分子分母同乘若干次 g , 使分母相同、分子也相同. 因此上述公式与分式表示无关; 通分后直接验证加法与莱布尼茨法则, 就得到了所需延拓.

由张量-Hom 伴随与微分模的泛性质, 对每个 B_g -模 M 有

$$\begin{aligned} \mathrm{Hom}_{B_g}(\Omega_{B/A}^1 \otimes_B B_g, M) &\simeq \mathrm{Hom}_B(\Omega_{B/A}^1, M) \\ &\simeq \mathrm{Der}_A(B, M) \simeq \mathrm{Der}_A(B_g, M). \end{aligned}$$

所以 $\Omega_{B_g/A}^1 \simeq \Omega_{B/A}^1 \otimes_B B_g$. 在几何上, 这正是把 $\mathrm{Spec} B$ 上的微分限制到主开集 $D(g)$. 缩小底空间时也相容: 若 $s \in A$ 的像在 B_g 中可逆, 逆元微分公式表明, A -导子也消去 A_s 的像. 因而 B_g 上的 A -导子正是 A_s -导子, 故 $\Omega_{B_g/A_s}^1 \simeq \Omega_{B_g/A}^1$.

第九讲已介绍层与仿射概形. 若带环空间的每一点都有与仿射概形同构的开邻域, 就称它为概形. 在概形 X 上, 正则函数组成结构层 $\mathcal{O}_X$. 微分也可以按开集组织起来, 形成 $\mathcal{O}_X$ -模层: 它在每个开集 U 上给出 $\mathcal{O}_X(U)$ -模, 限制映射保持加法和函数乘法, 交叠处相等的局部截面能唯一粘合.

设 $f: X \rightarrow S$ 为概形态射. 它在每个映入仿射开集 $V = \mathrm{Spec} A \subset S$ 的仿射开集 $U = \mathrm{Spec} B \subset X$ 上, 由环同态 $A \rightarrow B$ 给出: 点按素理想的逆像映射, 函数沿此同态拉回; 这些描述与开集限制相容.

在 U 上取微分模 $\Omega_{B/A}^1$, 在主开集 $D(g)$ 上取 $\Omega_{B/A}^1 \otimes_B B_g$. 限制映射由函数环的限制同态通过张量积诱导; 对任意开集, 将主开集上的相容元素按层的规则粘合, 便得到 U 上的模层. 在不同仿射开集的交叠处取公共主开集覆盖, 局部化公式把两边的微分相互识别; 泛性质的唯一性保证这些识别在三重交叠处相容. 因此它们粘合成 X 上的相对余切层(relative cotangent sheaf), 记为 $\Omega_{X/S}^1$.⁹ 在 $U \times_V U = \mathrm{Spec}(B \otimes_A B)$ 中, 令 I 为对角线的理想, 即乘法同态的核; B -模 I/I^2 在 U 上给出的模层, 正是 $\Omega_{X/S}^1|_U$.

记 $d: \mathcal{O}_X \rightarrow \Omega_{X/S}^1$ 为各开集上相容的求微分映射. 对任意 $\mathcal{O}_X$ -模层 $\mathcal{F}$, 设 $\mathrm{Der}_S(\mathcal{O}_X, \mathcal{F})$ 表示保持限制、满足莱布尼茨法则并消去从 S 拉回的局部函数的加法映射, 则泛性质写为

$$\mathrm{Hom}_{\mathcal{O}_X}(\Omega_{X/S}^1, \mathcal{F}) \simeq \mathrm{Der}_S(\mathcal{O}_X, \mathcal{F}), \quad \ell \mapsto \ell \circ d.$$

⁹A. Grothendieck(与 J. Dieudonné 合作), *Éléments de géométrie algébrique IV*, 第四部分: 定义 16.3.1 及仿射解释 16.3.7, 第 14–15 页; 任意模层的导子泛性质见命题 16.5.3, 第 28 页.

左端是 $\mathcal{O}_X$ -线性的层映射. 在各仿射开集上应用定理 6.33, 所得分解在交叠处因唯一性相同, 因而粘合成唯一的层映射.

这一构造适用于任意概形态射. 对 $U = \operatorname{Spec} B$ 中的点 p , 其剩余域为 $\kappa(p) = \operatorname{Frac}(B/\mathfrak{p})$. 余切层在该点的纤维是

$$\Omega_{B/A}^1 \otimes_B \kappa(p),$$

其维数取在 $\kappa(p)$ 上, 并且可以随点变化. 例如当 $\operatorname{char} k \neq 2$ 时, 抛物线投影的相对微分在原点的纤维是一维, 其他点的纤维为零.

Grothendieck 在 1961 年的 Cartan 研讨班报告中, 也用对角线构造复解析空间的相对微分层. 这一构造允许空间有奇点, 也允许其函数层含有幂零元.¹⁰ 光滑流形上, 一次微分形式所成的模也有相应的泛性质, 所考虑的导子须满足光滑链式法则.¹¹

6.2.10 选读: 分歧点与曲面的亏格

先看 $\mathbb{C}$ -代数同态 $\mathbb{C}[t] \rightarrow \mathbb{C}[x], t \mapsto x^e$, 其中 $e \geq 1$ 为整数. 对非零复数 t , 方程 $x^e = t$ 有 e 个不同的解; 当 t 趋向零时, 这些解都趋向原点. 相对于 $\mathbb{C}[t]$, 有 $d(x^e) = 0$, 即 $ex^{e-1}dx = 0$, 故与例 6.34 相同的计算给出

$$\Omega_{\mathbb{C}[x]/\mathbb{C}[t]}^1 \simeq (\mathbb{C}[x]/(x^{e-1})) dx.$$

当 $e \geq 2$ 时, 整个微分模以 $dx, x dx, \dots, x^{e-2}dx$ 为复向量空间的基, 维数为 $e - 1$, 恰是导数在原点的零点阶数. 而它在原点的纤维还要模去 x , 只剩一维; 因此纤维维数本身不能区分不同的 $e \geq 2$. 当 $e = 1$ 时, 微分模为零.

对紧黎曼曲面, 这些局部重数与全局拓扑之间有一个精确关系. 设 $f: X \rightarrow Y$ 是连通紧黎曼曲面之间的非恒定全纯映射. 在 $p \in X$ 及 $f(p)$ 附近选局部坐标, 使映射写成 $w = z^{e_p}$; 正整数 e_p 称为 f 在 p 处的分歧指数, $e_p > 1$ 时称 p 为分歧点, 其像 $f(p)$ 称为分支值. 分歧点只有有限个, 避开分支值后, 每条纤维有相同的点数 d , 称为映射的次数. 记 g_X, g_Y 为两曲面的亏格, 即紧定向曲面的把手数. Riemann–Hurwitz 公式为

$$2g_X - 2 = d(2g_Y - 2) + \sum_{p \in X} (e_p - 1),$$

¹⁰A. Grothendieck, *Techniques de construction en géométrie analytique. VII. Étude locale des morphismes : éléments de calcul infinitésimal*, 报告 14, 1961 年 3 月 6, 20 日, 引言第 14-01 页及 §2 第 14-07–14-08 页. 解析版本使用全纯函数、解析纤维积及解析微分; 绝对情形对取值于干干解析层的导子的泛性质, 见 O. Riemenschneider, *复解析几何讲义*, §19.13, 定理 19.27, 第 610 页.

¹¹这里采用 C^∞ -导子, 即对每个光滑函数 $F: \mathbb{R}^n \rightarrow \mathbb{R}$ 都要求 $D(F(f_1, \dots, f_n)) = \sum_i (\partial_i F)(f_1, \dots, f_n) D(f_i)$. 它们由通常的余切丛刻画; 若只把光滑函数看作普通实代数, 则代数 Kähler 微分模通常更大. 见 D. Joyce, *Algebraic Geometry over C^∞ -rings*, §5.2, 定义 5.3、例 5.4 与注 5.5, 第 45–46 页.

和式中仅有限项非零. 修正项 $e_p - 1$ 是局部模型 $t = x^{e_p}$ 的相对微分模的复维数, 与前面计算一致.

这条公式可以从 Euler 示性数看出. 在 Y 上取三角剖分, 使顶点集包含全部分支值. 记顶点、边、面的数目为 V, E, F , 则其 Euler 示性数为 $\chi(Y) = V - E + F$. 提升到 X 后, 边和面的数目各乘以 d , 因为它们的内部避开分支值. 在一个顶点 q 上方, $\sum_{p \rightarrow q} e_p = d$, 所以不同顶点的数目比 d 少 $\sum_{p \rightarrow q} (e_p - 1)$. 从而

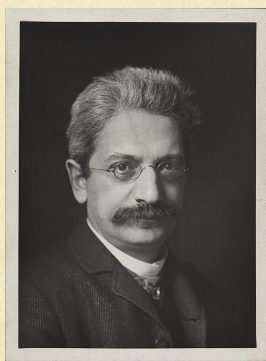
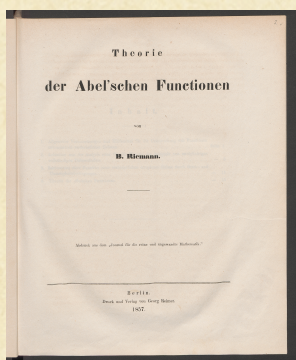
$$\chi(X) = d(V - E + F) - \sum_p (e_p - 1) = d\chi(Y) - \sum_p (e_p - 1).$$

代入连通紧定向曲面的基本公式 $\chi = 2 - 2g$, 便得到所述等式.

上一讲的椭圆曲线二叶覆盖 $E \rightarrow \mathbb{P}^1(\mathbb{C})$ 有四个分歧点, 其中 $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ 是黎曼球面. 每处 $e_p = 2$, 球面的亏格为零, 故 $2g_E - 2 = 2(-2) + 4 = 0$, 即 $g_E = 1$. 这与环面的拓扑模型一致.

同样, 给复数上的费马曲线 $r^n + s^n = 1 (n \geq 2)$ 补入 n 个无穷远点, 得到紧黎曼曲面; 投影到 r 给出到黎曼球面的 n 叶覆盖. 若 $r_0^n = 1$, 则 $1 - r^n$ 在 r_0 处为一阶零点; 由 $s^n = 1 - r^n$ 可知, s 是曲线的局部坐标, 而 $r - r_0$ 有 n 阶零点. 因而每个这样的值上方都有一个分歧指数为 n 的点. 绕 r_0 一周, s 的 n 个分支循环置换, 所以覆盖曲面连通. 在其余有限点, $s \neq 0$, 隐函数定理给出局部坐标 r , 没有分歧. 在无穷远处, 以 $u = 1/r$ 、 $v = s/r$ 为坐标, 方程为 $1 + v^n = u^n$, $u = 0$ 处的 n 个根互异, 各处都以 u 为局部坐标, 故也无分歧. 于是

$$2g - 2 = -2n + n(n - 1), \quad g = \frac{(n - 1)(n - 2)}{2}.$$



Riemann 在 1857 年的《阿贝尔函数论》中得到底曲面为球面时的亏格公式. Hurwitz 在 1891 年将底曲面推广到一般紧黎曼曲面, 并用 Euler 示性数证明了相应公式.

图 6.13: 左: Riemann《阿贝尔函数论》1857 年抽印本扉页. 中: Adolf Hurwitz (约 1892).¹²

¹²Riemann 的关系见 *Theorie der Abel'schen Functionen*, 1857 年抽印本, §7, 第 29 页; Hurwitz 的一般公式及证明见 *Ueber Riemann'sche Flächen mit gegebenen Verzweigungspunkten*, *Math. Ann.* 39 (1891), 第五部分 §2, 第 53–54 页. 书影: Berlin, Georg Reimer, 1857, ETH-Bibliothek Zürich, Rar 06, e-rara 数字原件. 肖像: 摄影者不详, 约 1892 年, ETH-Bibliothek, Portr 00852, 馆藏原图.

习题

- (1) 设 $r, s \in \mathbb{Q}$ 满足 $r^3 + s^3 = 1$. 证明 $r + s \neq 0$, 并令 $X = 12/(r + s)$, $Y = 36(r - s)/(r + s)$. 验证 $Y^2 = X^3 - 432$. 反过来, 给定满足 $Y^2 = X^3 - 432$ 且 $X \neq 0$ 的有理数 X, Y , 证明

$$r = \frac{36 + Y}{6X}, \quad s = \frac{36 - Y}{6X}$$

满足 $r^3 + s^3 = 1$, 且这两个变换互逆.

- (2) 列出方程 $y^2 = x^3 + x$ 在 $\mathbb{F}_5$ 中的所有解. 对环 $\mathbb{Z}[x, y]/(y^2 - x^3 - x)$, 写出与这些解对应的到 $\mathbb{F}_5$ 的环同态. 说明逐坐标模 5 如何把方程的整数解送到模 5 的解, 并计算 $(0, 0)$ 的像.
- (3) 设 A 为环, $n \geq 1$ 为整数, $B = A[x_1, \dots, x_n]$, M 为 B -模. 证明任一 A -导子 $D: B \rightarrow M$ 由 $D(x_1), \dots, D(x_n)$ 唯一决定, 且这 n 个值可以在 M 中任取. 由此证明 $\Omega_{B/A}^1$ 是以 $dx_1, \dots, dx_n$ 为基的自由 B -模.
- (4) 设 $\alpha: A \rightarrow B$ 为环同态, M 为 B -模. 在加法群 $B \oplus M$ 上定义 $(b, m)(c, n) = (bc, bn + cm)$, 并令 $a \mapsto (\alpha(a), 0)$. 验证这使 $B \oplus M$ 成为 A -代数. 记投影为 $\pi: B \oplus M \rightarrow B$. 证明满足 $\pi \circ s = \text{id}_B$ 的 A -代数同态 $s: B \rightarrow B \oplus M$, 与 $\text{Der}_A(B, M)$ 一一对应, 公式为 $s(b) = (b, D(b))$.
- (5) 设 k 为域, $B = k[x]/(x^n)$, 其中 $n \geq 2$, 仍以 x 表示商环中的元素. 用导子的泛性质证明 $\Omega_{B/k}^1 \simeq (B/(nx^{n-1}))dx$. 分别讨论 $\text{char } k \mid n$ 与 $\text{char } k \nmid n$ 的情况, 并计算它在点 $x = 0$ 处的纤维.
- (6) 设 k 为域, $A = k[t]$, $B = k[x]$, 并以 k -代数同态 $t \mapsto f(x)$ 赋予 B 以 A -代数结构, 其中 $f \in k[x]$. 证明 $\Omega_{B/A}^1 \simeq (B/(f'(x)))dx$. 对 $k = \mathbb{C}$, $f(x) = x^3 - 3x$, 求出微分模纤维非零的全部 $\mathbb{C}$ -值点 $x = a$, 并计算各纤维的维数.
- (7) 设 $B = \mathbb{R}[x, y]/(y^2 - x^3 + x)$, $p: B \rightarrow \mathbb{R}$ 为在 $(0, 0)$ 处取值的同态, $\mathfrak{m} = \ker p$. 分别从双数代入和 $\mathfrak{m}/\mathfrak{m}^2$ 计算点处切空间. 再求所有满足 $D(x) = 0$ 的点处导子, 并解释它们与投影到 x 轴的关系.
- (8) (选读) 设 $g \geq 0$ 为整数, $a_1, \dots, a_{2g+2}$ 是互异的复数. 考虑方程

$$y^2 = \prod_{i=1}^{2g+2} (x - a_i)$$

所对应的光滑紧黎曼曲面. 用坐标 $u = 1/x, v = y/x^{g+1}$ 说明无穷远处有两个点且投影无分歧, 再用 Riemann-Hurwitz 公式计算该曲面的亏格.