代数 2 H 课程讲义

Instructor: 余成龙
Notes Taker: 刘博文

Qiuzhen College, Tsinghua University
2022 Fall

课程信息:

- 授课人: 余成龙;
- 办公室: 近春园西楼 260;
- 邮箱: yuchenglong@mail.tsinghua.edu.cn;
- 成绩分布: 作业 (20%) + 期中 (30%) + 期末 (50%);
- 参考书: M.Atiyah *Communicative algebra*, S.Lang *Algebra*.

内容大纲:

- 伽罗瓦理论;
- 同调代数;
- 交换代数.

目录

第一部分

伽罗瓦理论

第一章　域论

1.1　域扩张

在本课程中, 如不加特殊说明, 环 R 总是指含有单位元的交换环, 并且环同态是保持单位元的.

定义 1.1.1. 对于环 R, 总有环同态 $\rho\colon \mathbb{Z} \to R$, 如果记 $\ker\rho = (n)$, 那么 R 的**特征** (characteristic)定义为 n.

定义 1.1.2. 如果环 R 中任何非零元素都可逆, 那么环 R 被称为一个**域** (field), 并且显然对于域来说, 其特征为素数.

我们在学习环论时, 环的理想是一个非常重要的概念, 但是对域来说, 其只有平凡理想, 即只有零理想及自身. 这很大程度上限制了域之间的同态, 假设有域同态 $\tau\colon E \to F$, 那么如果 τ 不是零映射, 那么 τ 一定是单射, 从而我们不妨将 E 视作包含在 F 中, 这引出了下面的概念.

定义 1.1.3. 给定域 E, F, 如果存在 (单) 同态 $\tau\colon F \to E$, 那么称 E 是域 F 的扩张 (extension), 记做 E/F.

注记. 当我们用 (单) 同态 τ 表示域扩张 E/F 时, 我们不仅强调我们可以将 F 视作 E 的子域, 也强调映射 τ 是如何映射的, 因为可能存在多种方式将 F 视作 E 的子域, 例如:

$$\begin{aligned} \tau\colon \mathbb{Q}[x]/(x^2+1) &\to \mathbb{C} & \tau'\colon \mathbb{Q}[x]/(x^2+1) &\to \mathbb{C} \\ x &\mapsto i & x &\mapsto -i \end{aligned}$$

都给出了这样的映射.

定义 1.1.4. 给定域扩张 E/F, 扩张的**次数** (degree)定义为 $[E:F] = \dim_F E$.

定义 1.1.5. 一个域扩张被称为**有限的** (finite extension), 如果其扩张次数有限, 否则被称为**无限的** (infinite extension).

命题 1.1.6. 对于域扩张 $F \subseteq E \subseteq K$, 则 $[K:F] = [K:E][E:F]$.

证明: 先假设 $E/F, K/E$ 都是有限扩张, 取 E 的一组 F-基 $\{\alpha_1, \dots, \alpha_n\}$ 以及 K 的一组 E-基 $\{\beta_1, \dots, \beta_m\}$, 那么简单的线性代数告诉我们 $\{\alpha_i\beta_j\}$ 是 K 的一组 F-基. □

例子. $\mathbb{C}/\mathbb{R}$ 是二次扩张, $\mathbb{R}/\mathbb{Q}$ 是无穷扩张.

例子. $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}/\mathbb{Q}$ 是二次扩张.

例子. 给定域 F, 考虑

$$F(x)=\{\frac{f(x)}{g(x)}\mid f(x),g(x)\in F[x]\}$$

则 $F(x)$ 是 F 的域扩张.

注记. 即任何域都可以找到一个更大的域作为其域扩张, 并且上述操作可以多次操作, 得到 $F(x,y),F(x,y,z)$ 等等.

定义 1.1.7. E/F 是域扩张, $S\subseteq K$ 是一个子集, 则记 $F[S]$ 是 E 中包含 F,S 的最小的子环; $F(S)$ 是 E 中包含 F,S 最小的子域. 特别地, 如果 $S=\{u\}$, 称 $F(u)$ 叫做域 F 的一个**单扩张** (simple extension).

命题 1.1.8. 假设域 $\mathbb{F}$ 的特征不为 2, 如果 E/F 是二次扩张, 那么 $E=F(\alpha)$, 其中 $\alpha^2\in F$.

证明: 假设 $\{1,\beta\}$ 是 E 的一组 F-基, 那么 $\beta^2=a+b\beta$, 其中 $a,b\in F$, 注意到

$$(\beta-\frac{1}{2}b)^2=a+\frac{1}{4}b^2\in F$$

那么 $\alpha=\beta-\frac{1}{2}$ 即可. □

注记. 域的特征不为 2 用在了配方上, 这是一个不可缺少的条件.

问题 1.1.9. 特征 2 域上的二次扩张是什么样的?

研究域扩张的一个重要的好处就是可以帮助我们求解方程, 例如 $x^2+1=0$ 在 $\mathbb{R}$ 上没有根, 但是我们可以在 $\mathbb{R}$ 的域扩张 $\mathbb{C}$ 中找到它的一个根, 实际上, 我们总可以通过域扩张的办法去寻找根.

命题 1.1.10. 给定域 F 以及多项式 $f(x)\in F[x]$, 存在域扩张 E/F 使得 $f(x)$ 在 E 中有根.

证明: 将 $f(x)$ 在 $F[x]$ 中写作不可约因子 $p_1(x)\dots p_k(x)$ 的乘积, 如果有一次因子, 那么 $f(x)$ 在 F 中就有根, 否则取某个不可约多项式 $p_1(x)$, 考虑

$$E=F[x]/(p_1(x))$$

那么 E/F 是一个域扩张, 并且 $f(x)$ 在 E 中有根 $x+(p_1(x))$. □

1.2 代数扩张

定义 1.2.1. $u\in E$ 称为在 F 上**代数** (algebraic), 如果存在非零多项式 $p(x)\in F[x]$, 使得 $p(u)=0$, 否则则称 u 在 F 上**超越** (transcendental).

例子. $\sqrt{2}$ 在 $\mathbb{Q}$ 上是代数元, e,π 在 $\mathbb{R}$ 上是超越元.

定义 1.2.2. 给定域扩张 E/F, $\alpha\in E$ 在 F 上代数, 则满足 $f(\alpha)=0$ 的次数最低的首一多项式 $f(x)$ 称为 α 的**极小多项式** (minimal polynomial).

注记. 我们还可以如下刻画 α 是否在 F 上代数: 考虑赋值映射 $\theta_u:F[x]\twoheadrightarrow F[\alpha]$, 则 α 在 F 上代数当且仅当 $\ker\theta_\alpha\neq 0$; α 在 F 上超越当且仅当 $\ker\theta_\alpha=0$, 即 θ_α 是一个同构.

命题 1.2.3. 给定域扩张 E/F, $\alpha \in E$ 在 F 上代数, $p(x)$ 是其极小多项式, 那么 $[F(\alpha):F] = \deg p(x)$.

证明: 注意到 $F(\alpha) \cong F[x]/(p(x))$, 并且 $[F[x]/(p(x)):F] = \deg p(x)$. □

引理 1.2.4. $F(\alpha)/F$ 是单扩张, α 在 F 上代数, $p(x)$ 是其极小多项式, 如果 E/F 是域扩张, $\beta \in E$ 使得 $p(\beta) = 0$, 则存在 F 嵌入 $\tau: F(\alpha) \hookrightarrow E$ 使得 $\tau(\alpha) = \beta, \tau|_F = \mathrm{id}$.

证明: 注意到 $F(\alpha) \cong F[x]/(p(x))$, 考虑如下交换图即可:

$$\begin{array}{ccc} F[x] & \longrightarrow & E \\ \downarrow & \nearrow & \\ F[x]/(p(x)) & & \end{array}$$

□

定义 1.2.5. 域扩张 E/F 称为**代数扩张** (algebraic extension), 如果 E 中任何一个元素都在 F 上代数, 否则称为**超越扩张** (transcendental extension).

例子. $\mathbb{C}/\mathbb{R}$ 是代数扩张.

命题 1.2.6. 有限扩张是代数扩张.

证明: 假设 E/F 是有限扩张, 任取 $\alpha \in E$, 考虑 $1, \alpha, \alpha^2, \ldots$, 由于 E/F 是有限扩张, 则存在足够大的 n 使得

$$\alpha^{n+1} = a_n\alpha^n + \cdots + a_1\alpha + a_0$$

从而 $\alpha \in E$ 在 F 上代数, 即 E/F 是代数扩张. □

注记. 反之并不成立, 即代数扩张不一定是有限扩张.

推论 1.2.7. 给定域扩张 E/F, 如果 $\alpha, \beta \in E$ 都在 F 上代数, 则 $\alpha \pm \beta, \alpha\beta, \alpha/\beta(\beta \neq 0)$ 都在 F 上代数.

证明: 由于 $\alpha, \beta \in E$ 都是代数的, 那么 $F(\alpha), F(\beta)$ 都是有限扩张, 从而 $F(\alpha, \beta)$ 也是有限扩张, 从而是代数扩张, 即 $\alpha \pm \beta, \alpha\beta, \alpha/\beta(\beta \neq 0)$ 都是代数的. □

注记. 这也就是说 E 中所有在 F 上代数的元素组成了 E 的一个子域.

1.3 分裂域

定义 1.3.1. 给定域扩张 E/F, 多项式 $p(x) \in F[x]$ 在 E 中**分裂** (split), 如果 $p(x)$ 在 E 中可以写成:

$$p(x) = c\prod_{i=1}^{n}(x - \alpha_i)$$

其中 $\alpha_i \in E$.

定义 1.3.2. 给定域扩张 E/F, E 被称作是 $p(x) \in F[x]$ 的**分裂域** (splitting field), 如果 E 是包含 F 使得 $p(x)$ 分裂的最小的域.

定理 1.3.3. *多项式 $p(x) \in F[x]$ 的分裂域 E 存在, 并在在同构意义下唯一. 并且 $[E:F] \leq n!$, 其中 $n = \deg p(x)$.*

证明: 我们通过对 $p(x)$ 次数的归纳来证明存在唯一性, 当 $n = 1$ 的时候是显然的.

1. 存在性: 根据命题1.1.10, 总可以找到域扩张 F'/F 使得 $p(x)$ 在 F' 中有根, 因此 $p(x)$ 在 $F'[x]$ 中可以写成:
$$p(x) = (x-u)p_1(x), \quad \deg p_1(x) = n-1$$
因此利用归纳假设, 存在 $p_1(x)$ 在 F' 上的唯一的分裂域 E, 并且 $[E:F'] \leq (n-1)!$, 根据分裂域的定义自然有 E 也是 $p(x)$ 在 F 上的分裂域, 并且 $[E:F] = [E:F'][F':F] \leq (n-1)! \cdot n = n!$.
2. 唯一性: 如果 E' 是 $p(x)$ 在 F 上的另一个分裂域, 根据引理1.2.4, 存在嵌入 $F' \hookrightarrow E'$, 那么 E' 也应是 $p_1(x)$ 在 F' 上的分裂域, 因此 $E' \cong E$.

□

索引