

近世代数之一

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

- ① 《近世代数引论》，科大出版社
- ② M. Artin, 《Algebra》
- ③ J. Rotman, 《Galois Theory》

何为近世代数？

- ① 解线性方程组 — 线性代数
- ② 解一元高次方程 — 近世代数
- ③ 解多元高次方程 — 代数表示论

- ① 求根以及求根公式
 - $\Rightarrow$ 系数与（重）根的运算（域扩张）
 - $\Rightarrow$ 域的同构群（Galois群）
- ② 系数域通常是无限域，而Galois群是有限群！
- ③ Galois大定理（1831）：方程根式可解 $\Leftrightarrow$ Galois群可解
- ④ “求根公式”不再是核心问题！

- ① 求根以及求根公式
 - $\Rightarrow$ 系数与（重）根的运算（域扩张）
 - $\Rightarrow$ 域的自同构群（Galois群）
- ② 系数域通常是无限域，而Galois群是有限群！
- ③ Galois大定理（1831）：方程根式可解 $\Leftrightarrow$ Galois群可解
- ④ “求根公式”不再是核心问题！（谁还记得1545年的Cardano公式、Ferrari公式呢？）

- ① Évariste Galois档案 <http://www.galois-group.net>
- ② Alexander Grothendieck 《Long March Through Galois Theory》, pp.1600, 1978-82.
- ③ <https://grothendieck.umontpellier.fr/archives-grothendieck/>
- ④ 预印本网站 arxiv.org (Algebraic Geometry, Quantum Algebra, Representation Theory, Rings and Algebras ...)

课程计划

- ① 环论（重点：整环、商域与域扩张）
- ② 有限群论（重点：循环群与低阶对称群）
- ③ Galois理论与Galois大定理（重点：子域与子群的对应）

近世代数之二

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 集合与映射
- ② 等价关系
- ③ 二元运算

- ① 当代数学的基石 — 集合
- ② 数学的研究对象=带有“特定结构”的集合
- ③ 环=可以加和乘的集合；域=可以四则运算的集合

映射

- ① 定义：两映射 $f: X \rightarrow Y$ 与 $f': X' \rightarrow Y'$ 相等，若 $X = X'$, $Y = Y'$ 且 $f(x) = f'(x)$ 对任何 $x \in X$ 成立。
- ② 映射的复合，恒等映射
- ③ 映射 f 的像 $\text{Im } f$ 、单射、满射、双射
- ④ 单射的内蕴刻画？满射的内蕴刻画？双射的内蕴刻画？（element-free, that is, categorical!）
- ⑤ 典范分解： $f = i \circ \pi$ ，其中 π 为满射， i 为单射。

基本构造

设 X, Y 为集合。

- ① 无交并 $X \amalg Y$ (若 X, Y 恰均为某个集合的子集, 这区别于正常的并 $X \cup Y$)
- ② 笛卡尔积 $X \times Y$
- ③ 映射集合 $\text{Map}(X, Y)$
- ④ 例: 存在双射 $\text{Map}(X, \{0, 1\}) \simeq \mathcal{P}(X)$, 其中 $\mathcal{P}(X)$ 为 X 的幂集。

典范双射

设 X, Y, Z 为集合。

- ① 典范双射 $\text{Map}(X \amalg Y, Z) \simeq \text{Map}(X, Z) \times \text{Map}(Y, Z)$
- ② 典范双射 $\text{Map}(X, Y \times Z) \simeq \text{Map}(X, Y) \times \text{Map}(X, Z)$
- ③ 伴随双射：存在典范双射

$$\text{Map}(X \times Y, Z) \simeq \text{Map}(X, \text{Map}(Y, Z))$$

等价关系

设 X 为集。

- ① X 上的等价关系 $R \subseteq X \times X$: 满足自反性、对称性、传递性。
- ② 记号: $a \stackrel{R}{\sim} b \Leftrightarrow (a, b) \in R$
- ③ 等价类 $[a]$ 、等价类的代表元以及商映射 $X \rightarrow X/\sim$
- ④ 关于 R 的完全代表元系 (研究等价关系的最核心内容!!!)
- ⑤ 例: 奇偶性, 模3剩余...

等价关系=分拆=满射

设 X 为集。

- ① X 的分拆是指其幂集某个子集 $\{X_i \mid i \in I\} \subseteq \mathcal{P}(X)$ 满足：
非空、无交、覆盖。
- ② 等价关系=分拆 (hint: 等价类)
- ③ 分拆=满射(的左等价类) (hint: 考虑元素 y 的逆像 $f^{-1}(y)$)

映射基本定理

定理

设 $f: X \rightarrow Y$ 为映射, $\sim^f$ 为 X 上相应的等价关系。则 f 诱导双射

$$\bar{f}: X/\sim^f \xrightarrow{\sim} \text{Im } f, \quad [x] \mapsto f(x).$$

特别地, 若 f 为满射, 则 Y “本质上” 是 X 的商集。

二元运算

设 S 为集。

- ① 二元运算 $\psi: X \times S \rightarrow S, (x, y) \mapsto \psi(x, y)$
- ② 结合律 $\psi(\psi(x, y), z) = \psi(x, \psi(y, z))$
- ③ 记号约定: $\psi(x, y) = x \cdot y$ (later, even as xy)
- ④ WARNING: 运算结果 $x \cdot y$ 中不能恢复出 x 或 y , 因为 ψ 一般不是单射!

广义结合律

定理

设 $(S, \cdot)$ 如上, 满足结合律. 则对于任意 $n \geq 1$, 唯一存在 n 元运算

$$[-, -, \dots, -]: S \times S \times \dots \times S \longrightarrow S$$

满足下列条件:

- ① $[x] = x$
- ② $[x, y] = x \cdot y$
- ③ $[x_1, x_2, \dots, x_n] = [x_1, \dots, x_i] \cdot [x_{i+1}, \dots, x_n]$, 任意 $1 \leq i \leq n-1$.

近世代数之三

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 环的定义
- ② 整环与域

环

- ① 环=类似于 $\mathbb{Z}$ ，带上加法、减法和乘法
- ② 起源于D. Hilbert “Zahlring” 1897 (德语Ring意味an association; 又指cylcal behaviour in $\mathbb{Z}[\alpha]$ or $\mathbb{Z}_n$)
- ③ 公理化定义E. Noether 1921

环的定义

定义

环是指三元组 $(R, +, \cdot)$: 非空集合 R 、其上两个二元运算 $+$ 以及 $\cdot$, 分别称为加法和乘法, 使得下述八条公理成立:

$$(A1) \quad (a + b) + c = a + (b + c)$$

$$(A2) \quad a + b = b + a$$

$$(A3) \quad \text{有零元素 } 0_R$$

$$(A4) \quad \text{有负元}$$

$$(M1) \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

$$(M2) \quad \text{有幺元 } 1_R \text{ (又称单位元)}$$

$$(D1) \quad \text{分配律}$$

$$(D2) \quad \text{分配律}$$

定义的说明

- ① 我们仅考虑含么环
- ② 约定：三元组 $(R, +, \cdot)$ 简记为环 R
- ③ 环相等 $(R, +, \cdot) = (R', +', \cdot')$ 当且仅当集合相等 $R = R'$ ，且映射相等 $+ = +'$ 及 $\cdot = \cdot'$
- ④ 环 R 中的减法运算: $a - b := a + (-b)$, 加法的逆运算

基本例子

- ① 整数环 $\mathbb{Z} = (\mathbb{Z}, +, \cdot)$
- ② Gauss 整数环 $\mathbb{Z}[\sqrt{-1}]$
- ③ 一元多项式环 $\mathbb{Q}[x]$, x 为字母 (此处强调: x 为符号、不取值的未定元)
- ④ 同余类环 $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$, $n \geq 2$
- ⑤ 矩阵环 $M_n(\mathbb{C})$ (表示论课程!)

环的基本性质

定义：求和符合 $\sum_{i=1}^n a_i = a_1 + \cdots + a_n$

定义：定义 $0a = 0_R$; $n \geq 1, a \in R$, a 的 n 倍以及 $-n$ 倍分别定义为

$$na = a + \cdots + a, (-n)a = (-a) + \cdots + (-a)$$

WARNING: “倍乘”与 R 中乘法是完全不同的概念!

- ① 加法消去律 $a + b = a + c \Rightarrow a = c$
- ② $(n + m)a = na + ma$, 任意 $n, m \in \mathbb{Z}$
- ③ $na = (n1_R) \cdot a$, 特别地, $0_R \cdot a = 0_R$

命题

设 R 为环。则以下断言等价：

- ① $0_R = 1_R$;
- ② $R = \{0_R\}$;
- ③ R 仅含有一个元素。

此类环称为**零环**. 我们只考虑非零环。

二元环

例子

抽象定义二元环 $X = \{x_0, x_1\}$

加法表

+	x_0	x_1
x_0	x_0	x_1
x_1	x_1	x_0

乘法表

$\cdot$	x_0	x_1
x_0	x_0	x_0
x_1	x_0	x_1

尝试：如何验证 X 是环？

思考：环 X “本质上” 是模2同余类环 $\mathbb{Z}_2$

记号：均记为 $\mathbb{F}_2$ ，称二元域

二项式定理

称 R 为交换环, 若 $a \cdot b = b \cdot a$ 。

以后, 我们仅考虑含么交换环 R 。定义幂 $a^n = a \cdot a \cdots a$,
以及 $a^0 = 1_R$ 。

验证: $a^n \cdot a^m = a^{m+n}$

定理 (I. Newton 1665)

设 $a, b \in R$ 为环, $n \geq 1$ 。则有

$$(a + b)^n = \sum_{i=0}^n \binom{n}{i} a^i \cdot b^{n-i}.$$

可逆元

- ① $a \in R$ 称为乘法可逆元 (或单位), 若存在 b 满足 $a \cdot b = 1_R$.
- ② 记号 $b = a^{-1}$, 进而有 a^n , 任意 $n \in \mathbb{Z}$
- ③ 除法运算 $c \div a := c \cdot a^{-1}$, 即为乘法的逆运算

命题

设 $a \in R$ 可逆。则有

- ① $a^n \cdot a^m = a^{m+n}$
- ② 乘法消去率: $a \cdot x = a \cdot y \Rightarrow x = y$

单位群

- ① $U(R) = \{a \in R \mid a \text{可逆}\}$
- ② 验证: $U(R)$ 自然成为群, 称为环 R 的**单位群**
- ③ 试刻画 $U(\mathbb{Z})$, $U(\mathbb{Z}[\sqrt{-1}])$, $U(\mathbb{Q})$, $U(\mathbb{Z}_8)$

设 $u \in U(R)$ 。定义新的环 $R_u = (R, +, \circ)$, 其中新乘法为

$$a \circ b = u^{-1} \cdot a \cdot b$$

思考: R_u 与 R “本质”一样么?

整环与域

约定：乘法 $a \cdot b$ (有时)简记为 ab !

定义

非零环 R 称为整环，若 $ab = 0_R$ 蕴含 $a = 0_R$ 或 $b = 0_R$ ；非零环 R 称为域，若非零元均可逆。

- ① 整环中满足乘法消去率
- ② 域是整环
- ③ 域是可以做“四则运算”的环，也为解方程的操作区域!

例子

- ① $\mathbb{Z}, \mathbb{Z}[\sqrt{-1}]$ 是整环, 不是域
- ② $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 为域
- ③ 同余类环 $\mathbb{Z}_n$ 为整环 $\Leftrightarrow$ 其为域 $\Leftrightarrow n = p$ 为素数。此时, 记为 $\mathbb{F}_p$
- ④ $U(\mathbb{Z}_n) = \{[m] \mid \gcd(m, n) = 1\}$, 其阶为 $\phi(n)$, Euler 函数
试证明: 有限环 R 是整环 $\Leftrightarrow R$ 是域。

子环和子域

定义

(1) 设 R 为环。子集 $S \subseteq R$ 称为子环, 若满足 $1_R \in S$, S 对加法、减法以及乘法封闭。

(2) 设 K 为域。子环 $S \subseteq K$ 称为子域, 若满足 $0_R \neq a \in S$, 则 $a^{-1} \in S$, 即, 对除法也封闭。

- ① 子环自然成为环; 子域自身作为环是域。
- ② 这里的子环与课本上可能不同, 我们强烈要求 $1_R \in S$ 。
- ③ 平凡子环 $R \subseteq R$
- ④ 整环的子环是整环。
- ⑤ $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ 子环链

思考题：子环与子域

- ① $\mathbb{Z}$ 以及 $\mathbb{Z}_n$ 均没有真子环
- ② $\mathbb{Q}$ 以及 $\mathbb{F}_p$ 均没有真子域
- ③ 分类 $\mathbb{Z}[\sqrt{-1}]$ 的子环。(定义：两子环 $X, Y \subseteq \mathbb{Z}[\sqrt{-1}]$ 相等，若作为子集 $X = Y$ 。分类=完全列出)
- ④ 分类 $\mathbb{Q}$ 的子环。
- ⑤ 证明 $\mathbb{Q}(\sqrt{-1}) = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$ 是子域，并分类 $\mathbb{Q}(\sqrt{-1})$ 的子域。

近世代数之四

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 环同态
- ② 商环
- ③ 同态基本定理

环同态

定义

设 R, S 为环。映射 $\theta: R \rightarrow S$ 称为环同态, 若满足以下条件

- ① θ 保持加法和乘法
- ② $\theta(1_R) = 1_S$

双射的环同态称为环同构。

- ① 我们强烈要求环同态保持单位元(比较课本)!
- ② 同态的存在意味着“具有某种相同的性质和形态”。
例： $\mathbb{Q}$ 与 $\mathbb{Z}_n$ 之间无环同态； θ 诱导群同态 $\theta: U(R) \rightarrow U(S)$
- ③ 同态的复合；环同态的逆为环同构；环自同构群 $\text{Aut}(R)$
- ④ 同构的环“本质一样”，即具有相同的性质!

例子

- ① 恒等同态 $\text{Id}_R: R \rightarrow R$
- ② 设有子环 $S \subseteq R$ 。则包含映射 $\text{inc}: S \rightarrow R$
- ③ 对于任何环 R , 存在唯一的环同态 $\mathbb{Z} \rightarrow R$, 称为特征同态

环同态的像与等价关系

考虑环同态 $\theta: R \rightarrow S$

- ① 像 $\text{Im } \theta \subseteq S$ 为子环
- ② 相应的等价关系 $\sim^\theta$ 分析如下: $a \sim^\theta b$ 当且仅当 $\theta(a) = \theta(b)$
- ③ 这等价于 $a - b \in \theta^{-1}(0_R) = \text{Ker } \theta$, 称为 θ 的核
- ④ 相应的等价类 $[a] = \theta^{-1}(\theta(a)) = a + \text{Ker } \theta$, 核的“平移”
- ⑤ 故, 商集 $R/\sim^\theta$ 等于 $\{\text{Ker } \theta \text{ 的平移}\}$

核的特性

- ① 核 $\text{Ker}; \theta$ 完全确定了等价关系 $\sim$
- ② $\text{Ker}; \theta \subseteq R$ 对加法、减法和乘法封闭，但不是子环!!
- ③ 重要观察: $x \in \text{Ker } \theta$, 任意 $a \in R \Rightarrow ax \in \text{Ker } \theta$
- ④ 核对有 R 中求“倍元”封闭 (远强于: 乘法封闭性)

定义 (R. Dedekind 1871)

子集 $I \subseteq R$ 称为**理想**, 若 I 对加、减法以及倍元封闭。记号 $I \triangleleft R$

- ① 虽然 $R \triangleleft R$, 但我们通常仅考虑真理想 (理想 I 真当且仅当 $1_R \notin I$)。
- ② 平凡理想 $\{0_R\}$ 以及 R
- ③ 任意元素 $a \in R$ 给出**主理想** $(a) = aR = \{a \text{ 的倍元} \}$
- ④ 环 R 为域当且仅当 R 仅有平凡理想

同态核=理想

- ① 如上，环同态的核是真理想
- ② 给定 $I \triangleleft R$ ，定义商环 R/I 如下：
 - (1) 给出同余等价关系 $a \equiv b \pmod I$ 以及等价类 $\bar{a} = a + I$
 - (2) 其商集 $R/\equiv$ 记为 R/I ，自然定义其加法和乘法（重点：验证其定义合理性，即，与代表元选取无关）
- ③ 这完全模仿同余类环 $\mathbb{Z}_n$ 的构造，
即 $n\mathbb{Z} \triangleleft \mathbb{Z}$ 且 $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ ！（想法见于神C. Gauss 1801）
- ④ 练习：分类 $\mathbb{Z}$ 的所有理想。

典范同态的泛性质

考虑理想 $I \triangleleft R$ 。典范同态 $\text{can}: R \rightarrow R/I$, $a \mapsto \bar{a}$ 。则有 $\text{Ker can} = I$ 。

命题

设 $\theta: R \rightarrow S$ 为环同态。则 $I \subseteq \text{Ker } \theta$ 当且仅当 $\theta = \theta' \circ \text{can}$, 其中 $\theta': R/I \rightarrow S$ 为某个环同态。

此时, 同态 θ' 是唯一的, 由 θ 诱导的。

环同态基本定理

定理

设 $\theta: R \rightarrow S$ 为环同态。则唯一存在环同构

$$\bar{\theta}: R/\text{Ker } \theta \xrightarrow{\sim} \text{Im } \theta$$

使得下图交换

$$\begin{array}{ccc} R & \xrightarrow{\theta} & S \\ \text{can} \downarrow & & \uparrow \text{inc} \\ R/\text{Ker } \theta & \xrightarrow{\bar{\theta}} & \text{Im } \theta \end{array}$$

注： $\bar{\theta}(\bar{a}) = \theta(a)$ ，并比较之前的映射基本定理！

- ① 设 $\theta: R \rightarrow S$ 是单的。则有环同构 $R \simeq \text{Im } \theta$ ，即， R “等同于” S 的子环。（单的环同态又称为环嵌入）
- ② 设 $\theta: R \rightarrow S$ 是满的。则有环同构 $R/\text{Ker } \theta \simeq S$ ，即， S “等同于” R 的商环。
- ③ 特征映射 $\mathbb{Z} \rightarrow R$ ，其核为 $n\mathbb{Z}$ ，其中 $n = 0$ 或 $n \geq 2$ 。
记 $n = \text{char}(R)$ ，称为环 R 的特征
- ④ 整环的特征为0或素数 p

- ① 考虑 R 的两个理想 $I \subseteq J$ 以及典范同态

$$R/I \rightarrow R/J, \quad a + I \mapsto a + J.$$

- ② 其核为 $J/I = \{a + I \mid a \in J\}$, 且有诱导的环同构

$$(R/I)/(J/I) \simeq R/J, \quad \bar{a} + J/I \mapsto \bar{a}.$$

- ③ 存在双射

$$\{J \triangleleft R \mid I \subseteq J\} \longleftrightarrow \{R/I \text{ 的理想}\}, \quad J \mapsto J/I$$

- ④ 分类 $\mathbb{Z}_n$ 的理想!

近世代数之五

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 分式域
- ② 商域

分式域

- ① 回顾从 $\mathbb{Z}$ 到 $\mathbb{Q}$ 的构造
- ② 设 R 为整环。记 $R^\times = R \setminus \{0\}$ 。考虑集合 $R \times R^\times$ 上的关系

$$(a, x) \simeq (b, y) \text{ 当且仅当 } ay = bx$$

- ③ 相应的等价类记为，称为分式：

$$\frac{a}{x} = \{(b, y) \in R \times R^\times \mid (b, y) \simeq (a, x)\}$$

- ④ 分式的全体 $\text{Frac}(R) = R \times R^\times / \sim$

分式域, 续

- ① $\text{Frac}(R)$ 上自然定义加法和乘法

$$\frac{a}{x} + \frac{b}{y} = \frac{ay + bx}{xy}, \quad \frac{a}{x} \cdot \frac{b}{y} = \frac{ab}{xy}$$

- ② 定义合理性!
- ③ $\text{Frac}(R)$ 是域, 称为 R 的分式域

泛性质

考虑典范同态 $\text{can}_R: R \hookrightarrow \text{Frac}(R)$, $r \mapsto \frac{r}{1_R}$, 单射;
 can_R 是同构当且仅当 R 是域。

定理

设 R 为整环, K 为域。考虑环的单同态 $\phi: R \rightarrow K$ 。则存在唯一的域嵌入 $\tilde{\phi}: \text{Frac}(R) \rightarrow K$ 使得下图交换

$$\begin{array}{ccc} R & \xrightarrow{\text{can}_R} & \text{Frac}(R) \\ \phi \downarrow & & \nearrow \tilde{\phi} \\ K & & \end{array}$$

进一步, $\tilde{\phi}$ 是同构 $\Leftrightarrow$ 任意 $w \in K$ 均可表达为 $w = \phi(a)\phi(x)^{-1}$, 某些 $a, x \in R$ 。

例子

- ① $\mathbb{Z} \subseteq \mathbb{Q}$ 诱导 $\text{Frac}(\mathbb{Z}) \simeq \mathbb{Q}$
- ② $\mathbb{Z}[\sqrt{-1}] \subseteq \mathbb{Q}(\sqrt{-1})$ 诱导 $\text{Frac}(\mathbb{Z}[\sqrt{-1}]) \simeq \mathbb{Q}(\sqrt{-1})$
- ③ 设 F 为域。则 $\text{char}(F) = 0 \Leftrightarrow \mathbb{Q} \subseteq F$; 故, F 自然成为 $\mathbb{Q}$ -线性空间
- ④ $\text{char}(F) = p \Leftrightarrow \mathbb{F}_p \subseteq F$; 故, F 自然成为 $\mathbb{F}_p$ -线性空间

思考: 一般来说, 很难确定等价关系 $\sim$ 的完全代表元系, 故集合 $\text{Frac}(R)$ 难以琢磨....

素理想

定义

设 R 为环。真理想 $\mathfrak{p} \triangleleft R$ 称为**素理想**, 若 $ab \in \mathfrak{p}$ 蕴含着 $a \in \mathfrak{p}$ 或 $b \in \mathfrak{p}$ 。

- ① 设 $p \geq 1$ 。理想 $p\mathbb{Z} \triangleleft \mathbb{Z}$ 当且仅当 p 为素数
- ② $\mathfrak{p} \triangleleft R$ 为素理想当且仅当 $R/\mathfrak{p}$ 为整环
- ③ 零理想 $\{0_R\}$ 为素理想当且仅当 R 为整环
- ④ 环 R 的素谱 $\text{Spec}(R)$

极大理想与商域

定义

设 R 为环。真理想 $\mathfrak{m} \triangleleft R$ 称为极大理想, 若 $\mathfrak{m} \subseteq I \triangleleft R$ 蕴含 $\mathfrak{m} = I$ 或 $I = R$ 。

商域如下:

命题

真理性 $\mathfrak{m} \triangleleft R$ 是极大理想当且仅当 $R/\mathfrak{m}$ 为域。特别地, 极大理想是素理想。

- ① $\emptyset \neq \text{Max}(R) \subseteq \text{Spec}(R)$
- ② $\text{Max}(\mathbb{Z}) = \{p\mathbb{Z} \mid p \text{ 为素数}\}$

素元与不可约元

设 R 为整环。 $a \neq 0_R$ ，整除的记号 $a|b \Leftrightarrow b \in (a)$

定义

- ① 非零元 $a \in R$ 称为素元，若 (a) 为素理想，等价地， $a|xy$ 蕴含 $a|x$ 或 $a|y$
- ② 非零元 $a \in R$ 称为不可约元，若 a 非单位，且 $a = bc$ 蕴含着 b 或 c 是单位。

- ① 素元总不可约。
- ② 在 $\mathbb{Z}$ 中，素元=不可约元= $\pm p$ ， p 为素数
- ③ 在 $\mathbb{Z}[\sqrt{-3}]$ 中， $4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$ ， 2 不可约，但非素

课程展望

- ① 设 k 为域。考虑一元多项式环 $k[x]$ 。
- ② $k[x]$ 中的素元=不可约元，称为不可约多项式
- ③ 不可约多项式 $f(x)$ 生成的主理想 $(f(x)) \triangleleft k[x]$ 是极大的
- ④ 自然域同态 $k \rightarrow k[x]/(f(x)) = K$ ，域扩张
- ⑤ $f(x)$ 在 k 中无根，但 $f(x) \in K[x]$ 在 K 却有根，即 $\bar{x}$ 。添根构造，参见L. Kronecker 1887
- ⑥ 构造有限域E. Galois 1830

近世代数之六

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 一元多项式环
- ② 主理想整环PID
- ③ 不可约多项式
- ④ 添根构造

多项式

设 R 为环, x 为字母(形式符号)

① R 上关于 x 的多项式

$$f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$$

系数 $a_i \in R$, 其中的 $a_i x^i$ 为单项式

② 两多项式相等 $\Leftrightarrow$ 对应系数相等

③ 若 $a_n \neq 0_R$, 则称 $a_n x^n$ 为首项, a_n 为首项系数, 定义次数 $\deg(f) = n$; a_0 为常数项

④ 约定: $0_R x^i$ 可以略去, $1_R x^i$ 简记为 x^i

⑤ 多项式 $f(x)$ 称为首一的, 若 $a_n = 1_R$

一元多项式环

- ① $R[x]$ 自然成为环。
- ② 零多项式 0_R ，不定义次数；其他常值多项式 a 的次数定义为 0
- ③ 有典范环嵌入 $R \hookrightarrow R[x], a \mapsto a$
- ④ $x \in R[x]$ ，于是，单项式 x^i 恰等于 x 的第 i 次幂

$R[x]$ 的“另类定义”：考虑

$$\bar{R} = \{(a_0, a_1, \dots) \mid a_i \in R, a_i = 0_R \text{ when } i \gg 0\}$$

可以定义其上的加法和乘法使得

$$R[x] \simeq \bar{R}, \quad x \mapsto (0_R, 1_R, 0_R, \dots)$$

命题

若 R 为整环, 则 $R[x]$ 亦为整环。特别地, 若 k 为域, $k[x]$ 为整环。

注: $R[x]$ 绝不是域, 因为 $U(R[x]) \simeq U(R)$ 。

泛性质

命题

设 R 为环。对于任给的环同态 $\psi: R \rightarrow S$ 以及 $s \in S$, 则唯一存在环同态

$$\tilde{\psi}: R[x] \longrightarrow S$$

使得 $\tilde{\psi}|_R = \psi$ 且 $\psi(x) = s$.

例子

考虑 $\text{Id}_R: R \rightarrow R$ 以及 $a \in R$ 。则 a 处的赋值同态

$$\text{ev}_a: R[x] \longrightarrow R$$

使得 $f(x) \mapsto f(a)$, 称为多项式 $f(x)$ 在 a 处的取值。(强调: 这只是形象的说法, 不确切; 因为 $f(x)$ 不是函数, 故, 不能取值!)

例子, 续

例子

设 $f(x) \in R[x]$ 。则多项式 $f(x)$ 给出多项式函数

$$f: R \longrightarrow R, \quad a \mapsto f(a)$$

即, $f \in \text{Map}(R, R)$ 。强调: 函数 f 在 a 处 (真的可以) 取值!

定义函数环 $\text{Map}(R, R)$ 以及赋值同态

$$\text{ev}: R[x] \longrightarrow \text{Map}(R, R), \quad f(x) \mapsto f.$$

该映射一般不是单射。

不能混淆 $f(x)$ 以及 f , 它们根本不在同一集合里!

带余除法

回顾：初等数论的基石 — $\mathbb{Z}$ 上的带余除法

从现在开始， k 为域。（首一化： $f(x) = a \cdot \bar{f}(x)$ ，其中 a 为首项系数， $\bar{f}(x)$ 为首一多项式）

定理

给定多项式 $f(x)$ 以及非零多项式 $h(x)$ 。则存在多项式 $q(x), r(x) \in k[x]$ 使得

$$f(x) = q(x) \cdot h(x) + r(x)$$

且 $r(x) = 0$ 或 $\deg(r) < \deg(h)$ 。这样的 $q(x)$ 与 $r(x)$ 是唯一的。

注： $h(x) | f(x)$ 当且仅当 $r(x) = 0$ 。

余数定理

定理

给定多项式 $f(x)$ 以及 $a \in k$ 。则唯一存在存在多项式 $q(x) \in k[x]$ 使得

$$f(x) = q(x) \cdot (x - a) + f(a).$$

特别地, $(x - a) | f(x)$ 当且仅当 $f(a) = 0_k$ 。

展望: **解集** $\text{Root}_k(f) = \{a \in k \mid f(a) = 0_k\}$ 本质上是 $f(x)$ 的“线性因子”。

主理想整环PID

定义

整环 R 称为**PID**，若其任何理想均为主理想。

注：按定义，域为PID。但，我们仅考虑非域的PID。

定理

$\mathbb{Z}$ 以及 $k[x]$ 均为PID。

证明：利用带余除法。数的绝对值vs多项式的次数！

PID的基本性质

设 R 为整环。利用整除关系，定义最大公因子 $\gcd(a, b)$ （不一定存在）。

PID满足如下：

- ① 任何非零元素 a, b ，存在 $\gcd(a, b)$
- ② 存在Bezout等式
- ③ 素元=不可约元
- ④ 任何非零素理想均极大。故， $\text{Spec}(R) = \{0\} \cup \text{Max}(R)$ 。

最大公因式与不可约多项式

在 $k[x]$ ，我们可以约定：仅考虑首一多项式

例如：多项式 $f(x), g(x) \in k[x]$ ，其最大公因式是指首一多项式 $h(x)$ 满足： $h|f, h|g$ ，且若 $a(x)|f, a(x)|g$ ，总有 $h|a(x)$ 。

例如： $k[x]$ 中不可约元称为域 k 上的不可约多项式，故

$$\text{Max}(k[x]) \longleftrightarrow \{k \text{ 上首一不可约多项式} \}$$

特别地， $k \hookrightarrow \text{Max}(k[x]), \quad \lambda \mapsto (x - \lambda)$ 。

域扩张

设有域的包含关系 $k \subseteq K$ 。则 $f(x) \in k[x]$ 可视为 $K[x]$ 中元素。

- ① $\text{Root}_k(f) \subseteq \text{Root}_K(f)$
- ② $f(x) \in k[x]$ 不可约 $\nRightarrow f(x) \in K[x]$ 不可约
- ③ 设 $f(x), g(x) \in k[x]$ 。但，总有 $\gcd_{k[x]}(f, g) = \gcd_{K[x]}(f, g)$

思考：若域扩张 $\theta: k \hookrightarrow K$ （域同态一定是单的），相应的结果呢？

添根构造

设 k 为域, $f(x) \in k[x]$ 为首一不可约多项式。注意:
若 $\deg(f) \geq 2$, 则 $\text{Root}_k(f) = \emptyset$ 。

构造

考虑典范同态

$$\theta: k \xrightarrow{\text{can}} k[x] \xrightarrow{\text{can}} k[x]/(f(x)) = K$$

仍记 $\theta(\lambda) = \lambda + (f(x))$ 为 λ , 于是, 我们有 $k \subseteq K$ (**危险否?**)
记 $u = x + (f(x)) \in K$, **务必忘记**上面的符号 x , 被 $u \in K$ 取代!
视 $f(x) \in K[x]$, 有**重要观察**: $u \in \text{Root}_K(f)$, 即, $f(u) = 0_K$ 。

$$f(x) = (x - u) \cdot g(x)$$

其中 $g(x) \in K[x]$, 次数降低。探究 k -线性空间 K 的维数, 基。

泛性质

考虑 $\theta: k \hookrightarrow K = k[x]/(f(x))$ 如上。

定理

任给域同态 $\delta: k \rightarrow F$ ，以及 $\alpha \in F$ 满足 $\delta(f)(\alpha) = 0_F$ 。则唯一存在域同态

$$\delta': K \longrightarrow F$$

使得 $\delta = \delta' \circ \theta$ 以及 $\delta'(u) = \alpha$ 。

注： $\delta(f) \in F[x]$ ；等式 $\delta = \delta' \circ \theta$ 意味着 δ' 延拓 δ 。

例子

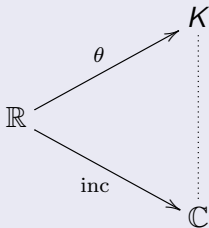
例子

考虑不可约多项式 $x^2 + 1 \in \mathbb{R}[x]$, 以及域嵌入

$$\theta: \mathbb{R} \longrightarrow \mathbb{R}[x]/(x^2 + 1) = K$$

记 $u = x + (x^2 + 1) \in K$ 。则 K 中元素为 $a + bu$, 其中 $a, b \in \mathbb{R}$ 。

探求: K 与 $\mathbb{C}$ 的关系, 更确切的, 两同态的关系



四元域

记 $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$ 。

例子

考虑不可约多项式 $x^2 + x + \bar{1} \in \mathbb{F}_2[x]$ ，以及域同态

$$\mathbb{F}_2 \hookrightarrow \mathbb{F}_2[x]/(x^2 + x + \bar{1}) = \mathbb{F}_4$$

记 $u = x + (x^2 + x + \bar{1}) \in \mathbb{F}_4$ (并忘记 x 与 $\mathbb{F}_4$ 的关系)。

探求: $\mathbb{F}_4$ 的加法表与乘法表。

解方程: 在 $\mathbb{F}_4$ 中解方程 $x^2 + x + \bar{1} = \bar{0}$ 。

比较: $\mathbb{F}_4$ 与 $\mathbb{Z}_4$

九元域

记 $\mathbb{F}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ 。

例子

考虑不可约多项式 $x^2 + \bar{1} \in \mathbb{F}_3[x]$ ，以及域同态

$$\mathbb{F}_3 \hookrightarrow \mathbb{F}_3[x]/(x^2 + \bar{1}) = \mathbb{F}_9$$

记 $v = x + (x^2 + \bar{1}) \in \mathbb{F}_9$ (并忘记 x 与 $\mathbb{F}_9$ 的关系)。

探求: $\mathbb{F}_9$ 的加法表与乘法表。

解方程: 在 $\mathbb{F}_9$ 中解 $x^2 + \bar{1} = \bar{0}$ 。

比较: $\mathbb{F}_4$ 与 $\mathbb{Z}_9$

近世代数之七

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- 1 欧式整环ED
- 2 例子

欧式整环

考虑整环 R , 以及 $R^\times = R \setminus \{0_R\}$ 。

定义

整环 R 称为**ED**, 若存在 *size function*

$$\phi: R^\times \longrightarrow \{0, 1, 2, \dots\}$$

使得任给 $a, b \in R^\times$, 存在 $q, r \in R$ 满足

$$a = qb + r$$

其中 $r = 0_R$ 或 $\phi(r) < \phi(b)$ 。

上表达式不唯一: $33 = 3 \cdot 9 + 6 = 4 \cdot 9 - 3$ (第二个更好, 因为 $\phi(-3) = |-3|$ 更小)。

ED是PID

定理

ED 是 PID 。

注: `size function`给出辗转相除法。

回顾 $\mathbb{Z}[\sqrt{-1}] = \{m + n\sqrt{-1} \mid m, n \in \mathbb{Z}\}$ 。

定理

$\mathbb{Z}[\sqrt{-1}]$ 是 ED, 从而是 PID。

证明: The norm map

$$N: \mathbb{Q}[\sqrt{-1}]^\times \longrightarrow \mathbb{Q}_+, \quad z \mapsto z \cdot \bar{z}$$

是乘法映射, 限制为 size function。需分析余项 $a + b\sqrt{-1}$, $|a|, |b| \leq \frac{1}{2}$ 。

证明: $U(\mathbb{Z}[\sqrt{-1}]) = \{\pm 1, \pm\sqrt{-1}\}$ 。

练习: 记 $i = \sqrt{-1}$ 。计算 $\gcd(4 + 7i, 3 + 4i)$ 。

回顾 $\mathbb{Z}[\sqrt{-2}] = \{m + n\sqrt{-2} \mid m, n \in \mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{-2})$ 。

定理

$\mathbb{Z}[\sqrt{-2}]$ 是 ED, 从而是 PID。

证明: The norm map

$$N: \mathbb{Q}[\sqrt{-2}]^\times \longrightarrow \mathbb{Q}_+, \quad z \mapsto z \cdot \bar{z}$$

是乘法映射, 限制为 size function。

证明: $U(\mathbb{Z}[\sqrt{-2}]) = \{\pm 1\}$ 。

$\mathbb{Z}[\sqrt{-3}]$ 不是PID

回顾 $\mathbb{Z}[\sqrt{-3}] = \{m + n\sqrt{-3} \mid m, n \in \mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{-3})$ 。

命题

$\mathbb{Z}[\sqrt{-3}]$ 不是PID。

证明： $2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$ ，2不可约，但非素元。

Eisenstein整数环

考虑 $\omega = e^{\frac{\pi i}{3}} = \frac{1+\sqrt{-3}}{2}$, 满足 $\omega^2 - \omega + 1 = 0$ 以及 $\omega^6 = 1$ 。

注意 $\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Z}[\omega] = \{m + n\omega \mid m, n \in \mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{-3})$ 。

定理

$\mathbb{Z}[\omega]$ 是ED, 从而是PID。

证明: 还是用the norm map $N(z) = z \cdot \bar{z} \in \mathbb{Q}_+$, (根据 a, b 正负性, 可能需要调整 a, b) 分析余项

$$a + b\omega = \left(a + \frac{b}{2}\right) + \frac{b}{2}\omega$$

(尽可能小)的长度。

证明: $U(\mathbb{Z}[\omega]) = \{\pm 1, \pm \omega, \pm \omega^2\}$ 。

思考: 为什么 $\mathbb{Z}[\sqrt{-3}]$ 不, 但扩大后却可以??

展望：代数整数环，参考Atiyah-Macdonald

考虑 $\mathbb{Z} \subseteq R \subseteq F = \text{Frac}(R)$ 使得 $\mathbb{Q} \subseteq F$ 是有限维空间。

定义 (E. Kummer 1847)

$\alpha \in F$ 成为代数整数，若 α 满足首一的整系数方程。记 F 中代数整数全体为 $\mathcal{O}_F$ 。

重要事实： $\mathcal{O}_F$ 是子环，且 $\text{Frac}(\mathcal{O}_F) = F$ 。

命题

假设 $R \subseteq \mathcal{O}_F$ 。若 R 是PID (或更弱点，为UFD)。则 $R = \mathcal{O}_F$ 。

证明： R 为UFD蕴含着 R 整闭。但，根据定义，我们看出 $\mathcal{O}_F$ 为 R 的整闭包。

注意： $\mathcal{O}_F$ 总整闭 (Dedekind整环)，但不是UFD。

$\mathbb{Z}[\sqrt{2}]$ 是ED

回顾 $\mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ 。

定理

$\mathbb{Z}[\sqrt{2}]$ 是ED, 从而是PID。

证明: $m + n\sqrt{2} \mapsto |m^2 - 2n^2|!$

练习: $1 + \sqrt{2} \in U(\mathbb{Z}[\sqrt{2}])$, 从而 $U(\mathbb{Z}[\sqrt{2}])$ 为无限群。

练习: $\mathbb{Z}[\sqrt{3}]$? $\mathbb{Z}[\sqrt{5}]$?

链接: <https://oeis.org/A048981>

近世代数之八

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① Gauss素数
- ② 平方和问题

PID的极大理想

定义

整环 R 中非零元 a, b 称为相伴的, 若存在 $u \in U(R)$ 使得 $a = bu$ 。
这等价于 $(a) = (b)$ 。

相伴是等价关系。

命题

设 R 为PID。则存在双射

$$\{a \in R \mid \text{素元}\} / \text{相伴关系} \longleftrightarrow \text{Max}(R), \quad a \mapsto (a).$$

回顾, 此时 $\text{Spec}(R) = \{0\} \cup \text{Max}(R)$ 。

Gauss素数

Gauss整数环 $\mathbb{Z}[i]$ 中的素元称为**Gauss素数**。

回顾： $N(m + ni) = m^2 + n^2$ ，且 $N(m + ni) = 1$ 当且仅当 $m + ni \in U(\mathbb{Z}[i])$ 。

故， $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$ 。

于是， $m + ni$ 相伴于 $-m - ni$ ， $n - mi$ ，以及 $-n + mi$ 。

例子

$$2 = (1 + i)(1 - i) = (-i) \cdot (1 + i)^2$$

故，2不是Gauss素（相伴于“平方数”）。

练习： $1 + i$ 是Gauss素数。（考虑Norm）

引理

引理

设 $z \in \mathbb{Z}[i]$ 。若 $N(z) = p$ 为素数 (这样 p 只能是 2 或 $4k + 1$)，则 z 是 *Gauss* 素数。

引理

考虑奇素数 p 。若 $p = 4k + 3$ 。则 p 是 *Gauss* 素数。

证明: p 不可约: $p = x \cdot y$, 利用 norm map。

Fermat 二平方和定理1640

定理

设 p 为奇素数。则 $p = 4k + 1$ 当且仅当 $p = a^2 + b^2$ 。此时，这样的 a, b 唯一。

证明：“当”很容易。反过来，设 $p = 4k + 1$ 。则Euler判别法， $-\bar{1}$ 是模 p 二次剩余（或，利于循环群 $\mathbb{F}_p^\times$ 以及 $4|(p-1)$ ）。考虑环同构

$$\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[x]/(x^2 + \bar{1})$$

故， p 非素，故， $z|p$ 。则 $N(z) = p$ 且 $p = z \cdot \bar{z}$ ， z 素（ a, b 的唯一性可由 $\mathbb{Z}[i]$ 唯一分解得出）。

$p = 4k + 1$ 情况

如上, $p = 4k + 1$ 。则 $p = (a + bi)(a - bi)$, 且因子不相伴。

例如: $5 = 1^2 + 2^2$ 。故, 素元 $1 + 2i$ 以及 $1 - 2i$!

例如: $13 = 2^2 + 3^2$ 。故, 素元 $2 + 3i$ 以及 $2 - 3i$!

练习: 研究商域 $\mathbb{Z}[i]/(a + bi)$ 。

定理

在相伴的意义下, Gauss素数为以下:

- ① $1 + i$
- ② 素数 $p > 0$, 其中 $p = 4k + 3$
- ③ $a \pm bi$, 其中 $p = a^2 + b^2$ 为 $4k + 1$ 的素数, $0 < a < b$

注: $4k + 3$ 以及 $4k + 1$ 的素数均无穷个。

回顾: $\text{Spec}(\mathbb{Z}) = \{0\} \cup \{p\mathbb{Z} \mid p = 2, 3, 5, \dots\}$

任环同态 $\theta: R \rightarrow S$ 诱导 $\text{Spec}(S) \rightarrow \text{Spec}(R)$, $\mathfrak{q} \mapsto \theta^{-1}(\mathfrak{q})$

例子

研究 $\text{Spec}(\mathbb{Z}[i]) \rightarrow \text{Spec}(\mathbb{Z})$ 的图像。

这是满射, 研究其 *fibers*!

二平方和定理

定理

设 $n \geq 2$ 。则 n 可写成二平方和当且仅当有标准分解 $n = 2^r p_1^{m_1} \cdots p_t^{m_t}$ ，其中，若 $p_i = 4k + 3$ ，相应的 m_i 为偶数

证明：“当”比较容易（Fermat二平方和定理）。

反过来， $n = N(z)$ ，对 z 在 Gauss 整数环中做素因子分解（为什么可以做？用 Norm 归纳！）。

近世代数之九

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 唯一分解整环UFD
- ② Gauss定理

UFD的定义

定义

整环 R 称为**UFD**，若满足以下两条：

- ① 存在不可约分解: $a = c_1 c_2 \cdots c_r$, c_i 不可约
- ② 不可约分解唯一: $a = c'_1 c'_2 \cdots c'_s$, c'_j 不可约, 则 $r = s$ 且相差置换, c_i 与 c'_i 相伴。

命题

设 R 为 UFD 。则以下命题成立。

- ① 不可约元=素元。
- ② 存在gcd以及lcm
- ③ 标准分解 $a = up_1^{n_1} \cdots p_r^{n_r}$, p_i 素元, 两两不相伴; 从而, 可以给出 a 的所有因子(在相伴意义下)。

Noether环

设 $X \subseteq R$ 。则包含 X 的最小理想, 称为 X 生成的理想:

$$RX = \{ \text{有限和} \sum_i a_i \cdot x_i, \text{ 其中 } x_i \in X \}$$

若理想 I 由有限个元素生成, 则 I 称为有限生成理想。

定义

环 R 称为 **Noether环**, 若任何理想均有限生成。

例如, PID 是 Noether 环。事实上, 我们研究的环绝大多数是 Noether 环。

定理 (Hilbert 基定理 1890)

设 R 为 Noether 环。则 $R[x_1, \dots, x_n]$ 以及其商环均为 Noether 环。

Noether整环有不可约分解

不可约分解普遍存在!

命题

设 R 为Noether整环。则任何 $a \in R$ 有不可约分解。

素分解总唯一!

命题

设 R 为整环。若 a 有素分解。则其不可约分解唯一。

特别地, Noether整环 R 是UFD当且仅当: 不可约元=素元。

例如, PID是UFD。

虚二次域

定理 (Gauss 1801, Heegner 1952/ Baker 1966/ Stark 1967)

设 d 为square-free的正整数。则 $\mathbb{Q}(\sqrt{-d})$ 中的代数整数环 $\mathcal{O}$ 是UFD当且仅当是PID, 当且仅当 $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$ 。

注: $\mathcal{O}$ 是ED当且仅当 $d = 1, 2, 3, 7, 11$ 。

注: $\mathbb{Q}(\sqrt{d})$ 的情况更难; norm-ED完全分类[Hardy-Wright 1979]。

猜想(Gauss): 存在无穷个square-free的正整数 d 使得 $\mathbb{Q}[\sqrt{d}]$ 的代数整数环是PID。

Gauss定理

定理

设 R 为UFD。则 $R[x]$ 亦为UFD。

特别地， $\mathbb{Z}[x]$ 为UFD，不为PID (其素理想 (x) ，不极大)。

证明：定义容量 $c(f)$ 以及本原多项式。

引理 (Gauss引理)

设 $f(x), g(x) \in R[x]$ 。则 $c(f \cdot g) \sim c(f) \cdot c(g)$ ，其中 $\sim$ 表示相伴。
特别地，本原多项式之积仍是本原的。

考虑 $R[x] \subseteq K[x]$ ，其中 K 为分式域；利用 $K[x]$ 中已有的不可约分解。

得出 $R[x]$ 的两类不可约元： $a \in R$ 以及本原不可约多项式 $f(x) \in R[x]$ 。

两个有用的结论

相比于 $K[x]$ 中, 在 $R[x]$ 判别不可约通常较容易些。

命题

设 R 为 UFD , K 为其分式域。设 $f(x) \in R[x]$ 为本原多项式。则 $f(x) \in R[x]$ 不可约元当且仅当 $f(x) \in K[x]$ 为不可约多项式。

命题 (Eisentein判别法)

设 R 为 UFD , $f(x) = \sum_{i=0}^n a_i x^i \in R[x]$ 本原, $p \in R$ 素元。设 $p \nmid a_n$, $p \mid a_{n-1}, \dots, p \mid a_1$, $p^2 \nmid a_0$ 。则 $f(x) \in K[x]$ 不可约多项式。

例如, $x^n - 2 \in \mathbb{Q}[x]$ 均不可约。

近世代数之十

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 域扩张的概念
- ② 单扩张

域扩张

定义

域扩张是指域的同态 $\theta: k \hookrightarrow K$, 简记为 K/k 。

警告：记号 K/k 很危险！域扩张本质是同态 θ ，而此记号“真事隐”！

记号 K/k 的理由： $k \simeq \theta(k) \subseteq K$, k “等同”于 $\theta(k)$ ，后者为 K 的子域。于是，域扩张 $\theta: k \hookrightarrow K$ “等同”于包含映射 $\text{inc}: \theta(k) \hookrightarrow K$

所谓等同： $\lambda \in k$ “等同”于 $\theta(\lambda) \in \theta(k) \subseteq K$ 。

基本例子

例子

(1) 给定不可约多项式 $f(x) \in k[x]$, 考虑 $K = k[x]/(f(x))$, 令 $u = x + (f(x)) \in K$. 则有域扩张

$$k \hookrightarrow K, \quad \lambda \mapsto \lambda + (f(x))$$

右边的 λ 为常值多项式。

(2) 考虑 $k[x]$ 的分式域 $k(x)$, 称为有理函数域 (暂时, 它们还不是“函数”!). 则典范嵌入 $k[x] \hookrightarrow k(x)$ 诱导域扩张

$$k \hookrightarrow k(x), \quad \lambda \mapsto \frac{\lambda}{1}$$

域扩张的同构

比较两域扩张 $\theta: k \rightarrow K$ 以及 $\theta': k \rightarrow K'$?

定义

域扩张 θ 以及 θ' 之间的同构是指域同构 $\phi: K \rightarrow K'$ 使得 $\phi \circ \theta = \theta'$ 。

若 $\theta = \theta'$ ，则 θ 的自同构 $\phi: K \rightarrow K$ 又称为域扩张 K/k 的自同构。

于是， $\text{Aut}(K/k) \subseteq \text{Aut}(K)$ 为子群。

- ① 设 $R \subseteq S$ 为子环, $\alpha \in S$ 。记 $R[\alpha]$ 为包含 R 及 α 的最小子环
- ② 则有 $R[\alpha] = \{\sum r_i \alpha^i \mid \text{有限和 } r_i \in R\}$
- ③ 更一般地, 环的单同态 $\theta: R \hookrightarrow S$, 记 $R[\alpha] = \theta(R)[\alpha] \subseteq S$
- ④ 设 $k \subseteq K$ 为子域, $\alpha \in K$ 。记 $k(\alpha)$ 为包含 k 及 α 的最小子域
- ⑤ 则有 $k(\alpha) = \{(\sum r_i \alpha^i)(\sum r'_i \alpha^i)^{-1} \mid \text{所有可能}\}$
- ⑥ 域扩张 $\theta: k \hookrightarrow K$ 。同样 $k(\alpha) \subseteq K$ 以及 $k \hookrightarrow k(\alpha)$
- ⑦ 更多记号 $R[\alpha_1, \alpha_2], k(\alpha_1, \alpha_2)$

单扩张

定义

域扩张 K/k 称为单的, 若存在 $\alpha \in K$ 使得 $K = k(\alpha)$ 。

例子

- 1 添根构造 $k \hookrightarrow k[x]/(f(x))$
- 2 有理函数域 $k \subseteq k(x)$
- 3 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-1})$
- 4 $\mathbb{R} \subseteq \mathbb{C}$

代数元

定义

$\alpha \in K$ 在 k 上代数, 若存在非零 $f(x) \in k[x]$ 使得 $f(\alpha) = 0_K$ 。否则, 则称 α 为 k 上超越元。

- ① 限定词“ k 上”很关键。
- ② $\mathbb{C}/\mathbb{Q}$, 则 $\sqrt{2}, e^{\frac{2\pi i}{3}}$ 均为代数元
- ③ π (Lindermann 1882) 以及 e (Hermite 1873) 均为超越元
- ④ $k \subseteq k(x)$, 其中 x 在 k 上超越

最小多项式

定理

考虑 K/k 以及 $\alpha \in K$ 在 k 上代数。则唯一存在首一不可约多项式 $f(x) \in k[x]$ 满足:

- ① $f(\alpha) = 0$;
- ② 若 $g(x) \in k[x]$ 满足 $g(\alpha) = 0$, 则 $f(x) | g(x)$.

这样的多项式 $f(x)$ 称为 α 关于 k 的最小多项式。

证明: 考虑在 α 处的赋值同态

$$\text{ev}_\alpha: k[x] \longrightarrow K, \quad g(x) \mapsto g(\alpha)$$

考察其核。

练习

- ① 关于 $\mathbb{C}/\mathbb{Q}$, 计算 $\sqrt[3]{2}$, $\sqrt{2} + \sqrt{3}$ 的最小多项式
- ② 考虑域扩张 $\theta: k \rightarrow K$ 以及 $\theta': k \rightarrow K'$ 。若存在域扩张的同构 $\phi: K \rightarrow K'$ 满足 $\theta(\alpha) = \alpha'$ 。则 α 代数当且仅当 α' 代数, 且最小多项式一样。
- ③ 上例有助于体会条件“ $\phi \circ \theta = \theta'$ ”!

单扩张结构定理

定理

设有单扩张 K/k 使得 $K = k(\alpha)$ 。

- ① 若 α 代数，最小多项式 $f(x)$ ，次数为 d 。则：

$\dim_k K = d < \infty$ ，基为 $1, \alpha, \dots, \alpha^{d-1}$ 且 $K = k[\alpha]$ ；有域扩张同构 $K \simeq k[x]/(f(x))$ 。

- ② 若 α 超越。则 $\dim_k K = \infty$ ，且 $k[\alpha] \neq K$ ；有域扩张同构 $K \simeq k(x)$ 。

本质上仅有两种单扩张！我们主要研究有限维域扩张！

例子

例子

考虑 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, 有 $\mathbb{Q}$ -基 $1, \sqrt[3]{2}, \sqrt[3]{4}$ 。

考虑 $\mathbb{Q}(\sqrt[3]{2}\omega)/\mathbb{Q}$, 有 $\mathbb{Q}$ -基 $1, \sqrt[3]{2}\omega, \sqrt[3]{4}\omega^2$ 。

有域扩张同构

$$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q} \simeq \mathbb{Q}(\sqrt[3]{2}\omega)/\mathbb{Q}$$

强调, $\mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}(\sqrt[3]{2}\omega)$!

还有 $\mathbb{Q}(\sqrt[3]{2}\omega^2)/\mathbb{Q}$ 呢?

近世代数之十一

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 代数扩张
- ② 维数公式

代数扩张

定义

域扩张 K/k 称为代数扩张, 若任何 $\alpha \in K$ 均在 k 上代数。

引理

有限维域扩张总是代数扩张, 即, 若 $\dim_k K < \infty$, 则 K/k 代数。

维数公式

定理

考虑域扩张链 $k \subseteq K \subseteq E$ 。若 K/k 以及 E/K 为有限维扩张, 则 E/k 为有限维扩张。

$$\dim_k E = \dim_k K \cdot \dim_K E.$$

要点 (必须掌握): 利用 K/k 以及 E/K 的 (线性) 基构造 E/k 的基!

例子

给出 $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ 以及 $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ 的基, 其中 $\omega = e^{\frac{2\pi i}{3}}$!

练习: 设 K/k 为有限维扩张, $\alpha \in K$ 的最小多项式 $f(x) \in k[x]$ 。则 $\deg(f) \mid \dim_k K$!

有限生成代数扩张=有限维扩张

定理

域扩张 K/k 是有限维的 $\Leftrightarrow K/k$ 是有限生成的代数扩张。

要点：有限生成扩张是单扩张的“复合”

命题

考虑 $k \subseteq K \subseteq E$ 。则 E/k 代数 $\Leftrightarrow K/k$ 和 E/K 均代数。

代数闭包

考虑 K/k 。定义 $E = \{\alpha \in K \mid \alpha \text{ 在 } k \text{ 上代数}\}$ 。则 $E \subseteq K$ 为子域，称为 k 在 K 中的代数闭包。故， $k \subseteq E \subseteq K$ 且 K/E 无代数元。

例子

考虑 $\mathbb{Q} \subseteq \bar{\mathbb{Q}} \subseteq \mathbb{C}$ ，其中 $\mathbb{Q}$ 中元素称为代数数。注意： $\bar{\mathbb{Q}}$ 仍为可数域！

自同构群 $\text{Aut}(\bar{\mathbb{Q}}) = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ ， $\mathbb{Q}$ 的绝对**Galois**群，是现代代数数论中的中心研究对象。

近世代数之十二

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 域同态的延拓
- ② 分裂域

延拓同态

问题：考虑 E/k 及 E'/k' ，域嵌入 $\sigma: k \hookrightarrow k'$ 延拓至 $E \hookrightarrow E'$ ？

引理 (关键引理)

考虑下图， α/k 的最小多项式 $f(x) \in k[x]$

$$\begin{array}{ccc} \alpha \in E & & E' \\ \uparrow & & \uparrow \\ k & \xrightarrow{\sigma} & k' \end{array}$$

- ① 设 $\beta \in \text{Root}_E(\sigma(f))$ ，则唯一存在 σ 的延拓

$$\tilde{\sigma}: k(\alpha) \xrightarrow{\sim} k'(\beta) \subseteq E', \quad \alpha \mapsto \beta$$

- ② 恰好有 $|\text{Root}_E(\sigma(f))|$ 个这样的延拓。

分裂域

定义

多项式 $f(x) \in k[x]$ 的分裂域是指域扩张 K/k 满足:

- ① $f(x)$ 在 K 上分裂: $f(x) = (x - \alpha_1) \cdots (x - \alpha_n) \in K[x]$;
- ② $E = k(\alpha_1, \cdots, \alpha_n)$.

例子

设 $f(x) \in \mathbb{Q}[x]$. 利用代数基本定理:

$$f(x) = (x - z_1) \cdots (x - z_n), \quad z_i \in \mathbb{C}.$$

则 $E = \mathbb{Q}(z_1, \cdots, z_n)$ 为 $f(x)$ 的分裂域。

更多例子

例子

考虑 $x^2 + x + \bar{1} \in \mathbb{F}_2[x]$ 的分裂域！

例子

- ① 考虑 $x^2 + \bar{1} \in \mathbb{F}_3[x]$ 的分裂域！
- ② 考虑 $x^2 - x - \bar{1} \in \mathbb{F}_3[x]$ 的分裂域！

分裂域的唯一性

定理

给定域同构 $\sigma: k \xrightarrow{\sim} k'$, $f(x) \in k[x]$ 以及相应的 $\sigma(f) \in k'[x]$ 。
设 E/k 为 $f(x)$ 的分裂域, E'/k' 为 $\sigma(f)$ 的分裂域。则 σ 可延拓指
域同构

$$\delta: E \xrightarrow{\sim} E'.$$

这样的延拓至多有 $\dim_k E = \dim_{k'} E'$ 个!

证明: 对 $\dim_k E$ 归纳, 延拓至

$$k(\alpha_1) \xrightarrow{\sim} k'(\alpha'_1), \quad \alpha_1 \mapsto \alpha'_1$$

注意到 $E/k(\alpha_1)$ 为 $f(x) \in k(\alpha_1)[x]$ 的分裂域。

第一步延拓中: α'_1 至多有 $\dim_k k(\alpha_1)$ 个可能值!

分裂域的自同构

例子

考虑 $x^3 - 2 \in \mathbb{Q}[x]$, 其分裂域 $E = \mathbb{Q}(\omega, \sqrt[3]{2})$ 。

回顾 $\text{Aut}(E/\mathbb{Q}) = \text{Aut}(E)$ 。

利用延拓的方法具体给出其元素!

例子

考虑 $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + \bar{1})$ 的自同构

群 $\text{Aut}(\mathbb{F}_4) = \text{Aut}(\mathbb{F}_4/\mathbb{F}_2)$ 。

有重根的多项式

定义

非零多项式 $f(x) \in k[x]$ 称为**有重根**，若存在 E/k 使得有 $(x - a)^2 | f(x)$ ，某个 $a \in E$ 。

更严格说，在某个**扩域**里有重根。

内蕴刻画：引入**形式微分** $f'(x) \in k[x]$ 。

引理

$f(x) \in k[x]$ 有重根当前仅当 $\gcd_{k[x]}(f, f') = 1$ 。

可分多项式

定义

非零多项式 $f(x) \in k[x]$ 称为可分的, 若其 (在 $k[x]$ 中的) 不可约因子均无重根。

WARNING: $f(x)$ 的可分性与域 k 有关! 严格说, 域 k 上的多项式 $f(x)$ 可分

引理

若 $\text{char}(k) = 0$, 则任何多项式可分。

例子

考虑有理函数域 $k = \mathbb{F}_q(t)$ 。则 $x^p - t \in k[x]$ 不可约, 但有重根。故, $x^p - t \in k[x]$ 不可分。

可分性与自同构

定理 (续唯一性定理)

给定域同构 $\sigma: k \xrightarrow{\sim} k'$, $f(x) \in k[x]$ 以及相应的 $\sigma(f) \in k'[x]$ 。
设 E/k 为 $f(x)$ 的分裂域, E'/k' 为 $\sigma(f)$ 的分裂域。则多项式 $f(x) \in k[x]$ 可分当且仅当 σ 恰有 $\dim_k E$ 个延拓。此时, 我们有

$$|\operatorname{Aut}(E/k)| = \dim_k E.$$

证明: 回到唯一性定理的证明, 延拓!

- ① 若 E/k 是某个可分多项式 $f(x) \in k[x]$ 的分裂域，
则 $\text{Aut}(E/k)$ 记为 $\text{Gal}(E/k)$ ，称为 E/k 的**Galois 群**，也称为
方程 $f(x) = 0$ 的**Galois群**，又记为 $\text{Gal}_k(f)$ 。
- ② Galois理论：联系 $\text{Gal}(E/k)$ 的子群与 E 的子域。
- ③ 基于Galois理论，证明Galois大定理：
若 $\text{char}(k) = 0$ ， $f(x)$ 根式可解当且仅当 $\text{Gal}_k(f)$ 为可解群。

近世代数之十三

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 有限域
- ② 有限域的子域与自同构群

有限域的概念

设 E 为有限域 E 。

- ① $\text{char}(E) = p > 0$
- ② $\mathbb{F}_p \subseteq E$
- ③ 视 E 为 $\mathbb{F}_p$ -线性空间: $\bar{m}.a = ma$, 即 m 个 a 相加
- ④ 从而, $|E| = p^n$, 其中 $n = \dim_{\mathbb{F}_p} E$
- ⑤ p 元域必同构于 $\mathbb{F}_p$

Frobenius自同构

定义

有限域 E 上的**Frobenius**自同构 $\sigma: E \rightarrow E$ 定义为 $\sigma(a) = a^p$ 。

- ① Fermat小定理(1640): $\bar{n}^p = \bar{n}$
- ② 考虑 $\mathbb{F}_p(t)$, 其Frobenius自同态 $x \mapsto x^p$ 不是满射!

单位群

设 $|E| = p^n$ 。则单位群 $E^* = E \setminus \{0_E\}$ 满足 $|E^*| = p^n - 1$ 。

引理 (Lagrange定理的特殊情况!)

任何 $a \in E^*$, 我们有 $a^{p^n-1} = 1_E$ 。

故, 任何 $a \in E$ 均为 $x^{p^n} - x = \bar{0}$ 的根。

证明: 设有最小的 d 满足 $a^d = 1_E$ (why?)。考

虑 $H = \{1, a, \dots, a^d\}$ 以及 E^* 上的等价关系 $c \simeq d$, 若 $cd^{-1} \in H$ 。

考虑相应的分拆, 得出 $d | (p^n - 1)$

存在唯一性定理

定理

对于任何 n , 唯一存在 p^n 阶有限域。

通常记为 $\mathbb{F}_{p^n}$! (警告: 它只是“本质唯一”!)

证明: $\mathbb{F}_{p^n}$ 为 $x^{p^n} - x \in \mathbb{F}_p[x]$ 的分裂域!

特别地, 我们有

$$x^{p^n} - x = \prod_{a \in \mathbb{F}_{p^n}} (x - a).$$

$\mathbb{F}_p$ 上不可约多项式

命题

$$x^{p^n} - x = \prod_{d|n} \prod_{\{f(x) \in \mathbb{F}_p[x] \mid \text{monic irr. of degree } d\}} f(x)$$

证明：考虑 $x^{p^n} - x$ 的因子 $f(x)$ ，以及 $a \in \text{Root}_E(f)$ 。

则 $\mathbb{F}_p(a) \subseteq E$ ，维数公式。

反之，设 $g(x) \in \mathbb{F}_p[x]$ 为 d 次首一不可约。考虑其添根构造 $K = \mathbb{F}_p[x]/(g(x))$ 。则有 $g(x) \mid (x^{p^d} - x) \mid (x^{p^n} - x)$ 。

例子

例子 ($p = 2$)

$$x^4 - x = x(x + \bar{1})(x^2 + x + \bar{1})$$

$$x^8 - x = x(x + \bar{1})(x^3 + x^2 + \bar{1})(x^3 + x + \bar{1})$$

$$x^{16} - x =$$

$$x(x + \bar{1})(x^2 + x + \bar{1})(x^4 + x^3 + x^2 + x + \bar{1})(x^4 + x^3 + \bar{1})(x^4 + x + \bar{1}).$$

例子 ($p = 3$)

$$x^9 - x = x(x + \bar{1})(x - \bar{1})(x^2 + \bar{1})(x^2 + x - \bar{1})(x^2 - x - \bar{1})$$

取定 E 使得 $|E| = p^n$ 。

命题

- ① 设 $K \subseteq E$ 为子域。则 $|E| = p^d$ 且 $d|n$ 。
- ② 设 $d|n$ 。则存在唯一的子域 $K \subseteq E$ 满足 $|K| = p^d$ 。

考虑根集 $\text{Root}_E(x^{p^d} - x)$ 。

思考：尝试描述 E 的子域格（子域的包含关系!）

例子

$\mathbb{F}_{2^6}$ 的子域格。

生成元

设 $n = q_1^{r_1} \cdots q_t^{r_t}$ 。则 E 的极大真子域 K_i , 阶为 $p^{\frac{n}{q_i}}$ 。

命题

我们有 $\cup_{i=1}^t K_i \neq E$ 。故, 存在 $u \in E$ 满足 $E = \mathbb{F}_p(u)$ 。

- ① $\mathbb{F}_p[x]$ 上总有 n 次不可约多项式; 取 $f(x)$ 。
- ② 设 $u \in \text{Root}_E(f(x))$ 。则 $f(x) = \prod_{i=0}^{n-1} (x - \sigma^i(u))$ 。
- ③ 特别地, $\sigma^i(u) \neq u$, 对于 $1 \leq i \leq n-1$

自同构

注意 $\sigma \in \text{Aut}(E)$ 满足 $\sigma^n = \text{Id}_E$ 。

定理

$$\text{Aut}(E) = \{\text{Id}_E, \sigma, \dots, \sigma^{n-1}\}.$$

证明：考虑自同构 $\delta \in \text{Aut}(E)$ 在生成元 u 上的作用。

故, $\text{Aut}(E)$ 为循环群。考虑其子群...

有限域的Galois对应

设 E 为有限域, $|E| = p^n$ 。

定理 (有限域的Galois对应)

存在格的反同构

$$\{K \subseteq E \text{ 子域}\} \longleftrightarrow \{H \subseteq \text{Aut}(E) \text{ 子群}\}$$

使得 $K \mapsto \text{Aut}(E/K)$ 以

及 $H \mapsto E^H = \{a \in E \mid h(a) = a, \text{ for any } h \in H\}$

所有的子域和子群均具体给出。

注: 该处, 整数整除关系的两种不同“代数提升”!

近世代数之十四

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 单位根
- ② 分圆域

单位根

- ① 单位根 $w \in k$ 满足 $w^n = 1_k$ 。
- ② 单位根的阶 $\text{ord}(w) = d$: 最小的正整数 d 使得 $w^d = 1$ 。此时, 称 w 为 d 次本原单位根。
- ③ 设有 d 次本原单位根。则 $\text{char}(k) \nmid d$ 。

引理

设单位根 $w \in k$ 满足 $\text{ord}(w) = d$ 。则 $w^n = 1_k$ 当且仅当 $n|d$ 。

单位根的群

事实：若存在 d 次本原单位根 w 。

则 $\{1, w, \dots, w^{d-1}\} = \text{Root}_k(x^d - 1)$, 为 $k^\times$ 的 d 阶子群。

这是**唯一**可能的 d 阶子群。

定理

设 k 为（可能无限的）域，且 $H \subseteq k^\times$ 为 d 阶子群。则存在 d 次本原单位根 w ，且 $H = \{1, w, \dots, w^{d-1}\}$ 。

特别地，有限域的单位群 $\mathbb{F}_{p^n}^\times$ 是循环群。

复单位根

设 $n \geq 2$, 考虑 $\zeta = \zeta_n = e^{\frac{2\pi i}{n}}$ 。

则 $\text{Root}_{\mathbb{C}}(x^n - 1) = \{1, \zeta, \dots, \zeta^{n-1}\}$ 。

$$x^n - 1 = (x - 1)(x - \zeta) \cdots (x - \zeta^{n-1}).$$

引理

复 n 次本原单位根的全体恰为 $\{\zeta^d \mid 1 \leq d < n, \gcd(d, n) = 1\}$, 恰有 $\phi(n)$ 个。

分圆域

定义

分圆域 $\mathbb{Q}(\zeta)$, 等于 $x^n - 1 \in \mathbb{Q}[x]$ 的分裂域。

注意: $\mathbb{Q}(\zeta_2) = \mathbb{Q}$, $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$,
 $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\zeta_5)$

分圆多项式

定义

n 次分圆多项式

$$\Phi_n(x) = \prod_{\substack{w \\ n\text{次本原单位根}}} (x - w) = \prod_{\{1 \leq d < n \mid \gcd(d, n) = 1\}} (x - \zeta^d)$$

故, $\deg \Phi_n(x) = \phi(n)$ 。

分圆多项式的计算

补充定义 $\Phi_1(x) = x - 1$.

引理

$x^n - 1 = \prod_{d|n} \Phi_d(x)$ 。于是, $\Phi_n(x) \in \mathbb{Z}[x]$.

例子

$\Phi_2(x) = (x + 1)$, $\Phi_3(x) = x^2 + x + 1$, $\Phi_4(x) = x^2 + 1$,
 $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, $\Phi_6(x) = x^2 - x + 1$

不可约性

定理 (Gauss 1801/Kronecker 1854)

分圆多项式 $\Phi_n(x) \in \mathbb{Z}[x]$ 不可约。

从而，

定理

以下断言成立：

- ① $\dim_{\mathbb{Q}} \mathbb{Q}(\zeta_n) = \phi(n)$
- ② 存在群同构 $\text{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq U(\mathbb{Z}_n)$ ，满足 $\sigma \mapsto \bar{k}$ ，其中 $\sigma(\zeta) = \zeta^k$ 。

证明

例子 (特殊情况)

设 p 为素数。证明： $f(x) = 1 + x + \cdots + x^{p-1} = \frac{x^p - 1}{x - 1}$ 不可约。
考虑 $g(x) = f(x + 1)$ ，利用关于 p 的Eisenstein判别法。

例子 (一般情况)

考虑 n 次本原单位根 w 的最小多项式 $f(x)$ ，设 $p \nmid n$ 为素数。
断言 $f(w^p) = 0$ 。归纳，我们有 $f(w^{p_1 p_2 \cdots p_t}) = 0$ 。
为了证断言， w^p 的最小多项式为 $g(x) \in \mathbb{Z}[x]$ 。
故， $f(x) \cdot g(x) \mid \Phi_n(x)$ ，但 $f(x) \nmid g(x^p)$ 。
模 p 方法： $\mathbb{Z}[x] \mapsto \mathbb{F}_p[x]$ ，但 $x^n - \bar{1} \in \mathbb{F}_p[x]$ 无重根。

Kronecker-Weber 定理

定理 (Kronecker 1853-Weber 1886)

设 $K/\mathbb{Q}$ 为某个多项式的分裂域且 $\text{Aut}(K/\mathbb{Q})$ 为 *Abel* 群。则存在 n 以及子域 $L \subseteq \mathbb{Q}(\zeta_n)$ 使得 $K \simeq L$ 。

注：任何有限 *Abel* 群 G ，存在合适的 n 使得 $U(\mathbb{Z}_n) \twoheadrightarrow G$ 。

近世代数之十五

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 群的定义
- ② Lagrange定理
- ③ 元素的阶

群

定义

二元组 $(G, \cdot)$ 称为群, 其中 G 为非空集合, 乘法 “ $\cdot$ ” 为二元运算

$$G \times G \rightarrow G, \quad (a, b) \mapsto a \cdot b$$

满足如下:

(G1) 结合律 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(G2) 有么元 $1_G = 1$

(G3) 有逆元 (逆元唯一!)

注: 有时简记为群 G , 乘法运算 $a \cdot b = ab$

基本性质

引理

设 G 为群。

- ① 乘法消去率: $ab = ac \Rightarrow b = c$
- ② $(ab)^{-1} = b^{-1}a^{-1}$
- ③ 求逆运算 $(-)^{-1}: G \rightarrow G, \quad g \mapsto g^{-1}$ 为双射。
- ④ 对于任何整数 n , 定义幂次 a^n 。故, $a^{n+m} = a^n \cdot a^m$!

子群

定义

非空子集 H 称为子群, 若 $a \cdot b \in H$, $a^{-1} \in H$ 。记为 $H \leq G$ 。

平凡子群: $\{1_G\}$, G 。

基本例子:来自环

- ① 给定环 R , 自然有三个群: 加法群 $(R, +)$, 单位群 $(U(R), \cdot)$, 自同构群 $(\text{Aut}(Q), \circ)$
- ② 取 $R = \mathbb{Z}, \mathbb{Z}_n, \mathbb{Z}[i]$ 等
- ③ 考虑域扩张 K/k 。则 $\text{Aut}(K/k) \leq \text{Aut}(K)$

基本例子：群即对称

- ① 一般线性群 $GL(n, \mathbb{C})$
- ② 特殊线性群 $SL(n, \mathbb{C})$
- ③ $SO_n \leq O_n \leq GL(n, \mathbb{R})$
- ④ 考虑 $P \subseteq \mathbb{R}^n$, 图形 P 的对称群

$$\Sigma(P) = \{g \in SO_n(\text{或 } O_n) \mid g(P) = P\} \leq SO_n$$

基本例子：群即置换

- ① 抽象集 X ，其上的置换 $\sigma: X \rightarrow X$ 双射
- ② 对称群 $S(X) = \{X \text{ 上所有的置换}\}$
- ③ 例如： $\text{Aut}(R) \leq S(R)$
- ④ Cayley定理 (1878)：任何群“本质上”都是 $S(X)$ 的子群！

Lagrange 定理

若 $|G| < \infty$, 称为有限群.

定理

设 G 为有限群, $H \leq G$. 则: $|H|$ 整除 $|G|$.

是否想起: $k \subseteq E \subseteq K$, 则 $\dim_k E | \dim_k K$?

Lagrange 定理的证明

- ① $a \in G$, $aH = \{ah \mid h \in H\}$ 称为 H 的左陪集
- ② $Ha = \{ha \mid h \in H\}$ 称为 H 的右陪集
- ③ 左、右陪集都与 H 一样大，它们都是 G 上某个等价关系的等价类。
- ④ 若有分拆 $G = \bigcup_{i \in I} a_i H$, 则称 $\{a_i \mid i \in I\}$ 为 G 关于 H 的左陪集完全代表元系, $|I| = [G : H]$ 称为子群 H 的指数
- ⑤ 此时有, $G = \bigcup_{i \in I} Ha_i^{-1}$ 。故, $\{a_i^{-1} \mid i \in I\}$ 恰为关于 H 的右陪集完全代表元系

Lagrange 定理, revisited

定理

设 G 为有限群, $H \leq G$ 。则有

$$|G| = |H| \cdot [G : H]$$

类比: $k \subseteq E \subseteq K$, 则有

$$\dim_k K = \dim_k E \cdot \dim_E K!$$

元素的阶

定义

元素 $a \in G$ 的阶, 记为 $\text{ord}(a)$, 是指最小的正整数 d 使得 $a^d = 1_G$ 。若不存在这样的 d , 则记 $\text{ord}(a) = \infty$ 。

- ① 若 $|G| < \infty$, 则任何元素 a 具有有限的阶。
- ② 设 $\text{ord}(a) = d < \infty$ 。则 $a^n = 1_G$ 当且仅当 $d|n$ 。

阶 (续)

命题

设 $|G| > \infty$, $a \in G$ 。则

$$\text{ord}(a) \text{ 整数} \mid |G|$$

回想Fermat小定理: $a \in \mathbb{F}_p^\times$, $a^{p-1} \equiv 1 \pmod{p}$

群同态

定义

映射 $f: G \rightarrow G'$ 称为群同态, 若 $f(a \cdot b) = f(a) \cdot f(b)$ 。双射群同态称为群同构。

注: 群同态蕴含着 $f(1_G) = 1_{G'}$ 以及 $f(a)^{-1} = f(a^{-1})$ 。

例子

- ① 子群 $H \leq G$ 诱导包含同态 $\text{inc}: H \rightarrow G$
- ② $\det: \text{GL}(n, \mathbb{C}) \rightarrow \mathbb{C}^\times$
- ③ 单位根群 $\mu_n = \{z \in \mathbb{C} \mid z^n = 1\}$ 。则: 有群同构

$$\mu_n \simeq (\mathbb{Z}_n, +)$$

- ④ 群 $U(\mathbb{Z}_8)$ 与 μ_4 同构么?

群的直积

定义

设 G, H 为群。则 $G \times H$ 上有自然的群结构，称为其直积。

- ① 能找到 G 与 $G \times H$ 之间的自然同态么？
- ② 元素 (g, h) 的阶？
- ③ 设 R, S 为环。则 $U(R \times S) \simeq U(R) \times U(S)$ ！
- ④ $\mu_2 \times \mu_2$ 同构于 $U(\mathbb{Z}_8)$ ？**Klein** 四元群，记为 V_4 。

近世代数之十六

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

① 循环群

- ① 设 $X \subseteq G$ 。记 (X) 为包含 X 的最小子群，称为由 X 生成的子群。
- ② 问： (X) 中有哪些元素？
- ③ 若 $(X) = G$ ，则称 X 为 G 的生成元集。

循环群

定义

群 G 称为循环群, 若存在 $a \in G$ 满足 $\langle a \rangle = G$ 。此时, 称 a 为 G 的生成元。

例子

- 1 $\mathbb{Z}$, 生成元为1或者-1
- 2 $\mathbb{Z}_n$
- 3 μ_n

循环群的结构

命题

设 G 为循环群。则 G 同构于 $\mathbb{Z}$ 或 $\mathbb{Z}_n$ 。

命题

设 G 为循环群，生成元为 g 。

- ① 若 $|G| = \infty$ 。则 G 恰有两个生成元，且子群恰为 $\{1_G\}, (g^d)$, 任何 $d \geq 1$ ；每个子群均为循环群，均同构于 $\mathbb{Z}$, 也同构于 G 。
- ② 若 $|G| = n < \infty$ 。则恰有 $\phi(n)$ 个生成元 $\{g^k, \gcd(k, n) = 1\}$, 对于每个 $d|n$, 存在唯一的子群 H_d , 满足 $|H_d| = d$ 。

注: $n = \sum_{d|n} \phi(d)$, 因为 $\phi(d)$ 恰为 d 阶元的个数。

循环群的刻画

命题

n 阶群 G 为循环群当且仅当存在 n 阶元。特别地, p 阶群一定为循环群。

注: 这是第一个按阶数的群分类定理!

例: 群同构 $\mu_3 \times \mu_2 \simeq \mu_6$.

定理

设 $|G| = n < \infty$ 。则 G 为循环群 $\iff$ 任何 $d|n$, 至多存在唯一的 d 阶子群。

hint: 考虑 d 阶元的个数!

域单位群的子群

定理

设 k 为域, $G \leq k^\times$ 为有限子群。则 G 为循环群。

例子

考虑有限域 $E/\mathbb{F}_p$ 。则 $E^\times$ 为循环群, 特别地, $E/\mathbb{F}_p$ 为域的单扩张!

近世代数之十七

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 同态基本定理
- ② 正规子群

群同态

- ① 考虑群同态 $f: G \rightarrow G'$
- ② 像 $\text{Im}(f) \leq G'$ 是子群, 故, 其上有群结构
- ③ 等价关系: $a \sim^f b$ 当且仅当 $f(ab^{-1}) = 1_{G'}$, 也当且仅当 $f(b^{-1}a) = 1_{G'}$ 。

同态的核

定义

同态 $f: G \rightarrow G'$ 的核定义为 $\text{Ker}(f) = \{h \in G \mid f(h) = 1_{G'}\}$ 。显然, $\text{Ker}(f) \leq G$ 为子群。

注意: 令 $N = \text{Ker}(f)$ 。则 $a \stackrel{f}{\sim} b$ 当且仅当 $ab^{-1} \in N$, 也当且仅当 $b^{-1}a \in N$ 。故, $Nb = bN$, 也就是, N 的左右陪集重合!

正规子群

定义

子群 $N \leq G$ 称为正规子群, 若 $aN = Na$, 任意 $a \in G$ 。

- ① 若 G 为Abel群, 则任何子群均正规。
- ② 群 G 的中心 $Z(G)$ 是正规子群。
- ③ 同态核是正规子群。

- ① 设 $N \leq G$, $a \in G$ 。其共轭 $aNa^{-1} = \{axa^{-1} \mid x \in N\} \leq G$
- ② 存在群同构 $N \simeq aNa^{-1}$, 但作为子群, 通常不相等
- ③ 子群 $N \leq G$ 正规 $\iff N = aNa^{-1}$, 任何 $a \in G$

例子

$G = \text{GL}_2(\mathbb{F}_2) = \text{SL}_2(\mathbb{F}_2)$ 。

考虑 $\begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}$ 以及 $\begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{pmatrix}$ 生成的循环子群!

- ① 考虑正规子群 $N \triangleleft G$, 记左陪集集合

$$G/N = \{\bar{a} = aN \mid a \in G\}$$

- ② 定义乘法 $\bar{a} \cdot \bar{b} = \overline{ab}$. 问题: 定义合理性?
- ③ 典范同态 $\text{can}: G \rightarrow G/N$, 核为?

群同态基本定理

定理

考虑群同态 $f: G \rightarrow H$ 。则 f 唯一诱导群同构

$$\bar{f}: G/\text{Ker}(f) \xrightarrow{\sim} \text{Im}(f),$$

使得下图交换

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \text{can} \downarrow & & \uparrow \text{inc} \\ G/\text{Ker}(f) & \xrightarrow{\bar{f}} & \text{Im}(f) \end{array}$$

- ① f 单当且仅当 $\text{Ker}(f) = \{1_G\}$ 。此时, G 同构于 H 的子群。
- ② 若 f 满, 则 H 同构于 G 的商群。

例子

例子

考虑 $A = (1, 1), B = (-1, 1), C = (-1, -1), D = (1, -1)$ 围成的正方形 $\square \subseteq \mathbb{R}^2$ 。则有自然群同态

$$\Sigma(\square) \longrightarrow S(\{A, B, C, D\})$$

例子

考虑 $x^3 - 2 \in \mathbb{Q}[x]$ 的分裂域 $E/\mathbb{Q}$ ，及其根集 $X = \text{Root}_E(x^3 - 2) = \{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\}$ 。则有自然群同态

$$\text{Aut}(E/\mathbb{Q}) \longrightarrow S(X)$$

对应定理

定理

考虑 $N \triangleleft G$ 。则有双射

$$\{K \mid N \leq K \leq G\} \longleftrightarrow \{G/N \text{ 的子群}\}, K \mapsto K/N$$

我们有: $K \triangleleft G$ 当且仅当 $K/N \triangleleft G/N$, 此时有自然同构

$$(G/N)/(K/N) \xrightarrow{\sim} G/K.$$

同构定理

定理

设 $N \triangleleft G$, $H \leq G$ 。则 $NH = HN \leq G$, 且 $(H \cap N) \triangleleft H$, 有自然同构

$$H/(H \cap N) \xrightarrow{\sim} NH/N.$$

注：该定理不是重点！本节，群同态的例子是重点！

近世代数之十八

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 对称群
- ② 共轭类
- ③ 单群

对称群

命题

设有集合间双射 $\sigma: X \rightarrow Y$ 。则有群同构 $S(X) \simeq S(Y)$ 。

考虑 $\underline{n} = \{1, 2, \dots, n\}$ ，记 $S_n = S(\underline{n})$ ， n 元集合上的对称群，其运算为置换的符号。

注： S_1 为平凡群， $S_2 \simeq \mu_2$ 为 2 阶循环群。

记号

① $\sigma \in S_n$ 记为 $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$

② $\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$

例子

S_3 中: 考虑 $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ 以及 $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ 。计算 $\sigma\tau$ 以及 $\tau\sigma$

轮换

- ① 设 $i_1, i_2, \dots, i_t \in \underline{n}$ 两两不同, $t \geq 2$ 。定义 t -轮换

$$c = (i_1 i_2 \cdots i_t) \in S_n$$

如下: $i_1 \xrightarrow{c} i_2 \xrightarrow{c} \cdots \xrightarrow{c} i_t \xrightarrow{c} i_1$, 其他元素不动。

- ② 2-轮换称为对换
- ③ 1-轮换 (i) 均为恒等变换, 一般不考虑

引理

考虑轮换 σ, τ 。若它们不相交, 则 $\sigma\tau = \tau\sigma$!

引理

有用等式: $\sigma(i_1 i_2 \cdots i_t) \sigma^{-1} = (\sigma(i_1), \sigma(i_2), \dots, \sigma(i_t))$.

型与共轭类

命题

任何 $\sigma \in S_n$, 存在唯一的表达式 $\sigma = c_1 \cdots c_l$, 其中 c_i 为互不相交的轮换。

hint: 考虑 $\underline{n}$ 上的 σ -轨道!

定义 σ 的型 $1^{\lambda_1} 2^{\lambda_2} \cdots n^{\lambda_n}$, 满足 $\sum_{i=1}^n i \lambda_i = n$.

回顾: 群 G 中 a 与 b 共轭, 若存在 $g \in G$ 使得 $a = gbg^{-1}$; 这是等价关系, 其等价类称为共轭类。

定理

S_n 中两元素相互共轭 $\iff$ 它们同型!

例子

例子

- ① 具体给出 S_1, S_2, S_3, S_4 的共轭类
- ② 给出下面映射的像

$$\Sigma(\square) \longrightarrow S_4$$

交错群

引理

任何 $\sigma \in S_n$ 均能写成对换之积。

$$(ij) = (i+1, j)(i, i+1)(i+1, j)$$

故, S_n 由 $(12), (23), \dots, (n-1, n)$ 生成!

辫子关系

$$(i+1, i+2)(i, i+1)(i+1, i+2) = (i, i+1)(i+1, i+2)(i, i+1)$$

引理

存在群同态

$$S_n \longrightarrow \mathrm{GL}_n(\mathbb{R}), \quad \sigma \mapsto P_\sigma \text{ 置换方阵}$$

故, $\mathrm{sign}: S_n \rightarrow \{\pm 1\}$, 其核 A_n , n 元集合上的交错群

单群

定义

群 G 称为单群, 若没有非平凡的正规子群。

单群是群的building blocks, 但绝非简单的群!

定理

设 $n \geq 5$ 。则交错群 A_n 是单群!

第一步: A_n 由3-轮换生成。

第二步: 3-轮换在 A_n 中共轭。

第三步: 设 $N \triangleleft A_n$ 。则 N 包含某个3-轮换 (取 $x \in N$ 素数阶, 找适当的 $g \in A_n$ 使得 $gxg^{-1}x^{-1}$ 为3-轮换)。

对称群

命题

对称群 S_n 由 $(12), c = (1, 2, 3, \dots, n)$ 生成。

命题

对称群 S_5 可由仍给的对换和5-轮换生成！

hint: S_5 可由 c 以及 $(1i)$ 生成。

例子: A_4

例子

能否给出 A_4 的共轭类? 它是否有6阶子群?

近世代数之十九

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 群作用
- ② 共轭作用

群作用

定义

群 G (左边) 作用于集 X , 记为 $G \curvearrowright X$, 是指映射

$$\psi: G \times X \rightarrow X, \quad (g, x) \mapsto \psi(g, x) = g.x$$

满足:

① $1.x = x$

② $h.(g.x) = (hg).x$

此时, 称 X , 或 (X, ψ) , 为 G -集。

注: G -集 (X, ψ) 诱导群同态

$$\rho: G \rightarrow S(X), \quad g \mapsto \rho(g)$$

使得 $\rho(g)(x) = g.x$. 反之, 给定 ρ , 亦可定义 G -集。

轨道

给定 $G \curvearrowright X$, $x \in X$ 。

- ① x 的 G -轨道 $\mathcal{O}_x = G.x = \{g.x \mid g \in G\}$
- ② 可定义 X 上的等价关系：轨道为其等价类
- ③ 有无交并

$$X = \bigsqcup_{x \in I} \mathcal{O}_x,$$

称为 X 的轨道分解, I 为轨道的完全代表元系

- ④ 称群作用 $G \curvearrowright X$ 可迁的, 若只有一个轨道
- ⑤ 例如: 对于任何 $x \in X$, 总有限制的作用 $G \curvearrowright \mathcal{O}_x$; 它总是可迁的。

稳定化子

定义

考虑 $G \curvearrowright X$ 以及 $x \in X$ 。则 x 的稳定化子

$$G_x = \{g \in G \mid g(x) = x\} \leq G$$

引理

设 $x = h.y$ 。则 $G_x = hG_yh^{-1}$ 。故，同一轨道中的稳定化子是互相共轭的。

例子

- ① 设 $H \leq G$, 考虑 $G/H = \{aH \mid a \in G\}$ 。则 $G \curvearrowright (G/H)$, 左诱导作用。
- ② 特别地, $G \curvearrowright G$, 左正则作用
- ③ $S(X) \curvearrowright X$
- ④ 设 K/k 。则 $\text{Aut}(K/k) \curvearrowright K$ 。考虑 $f(x) \in k[x]$ 以及根集 $\text{Root}_K(f)$ 。则有作用

$$\text{Aut}(K/k) \curvearrowright \text{Root}_K(f)$$

注: Galois群本质上是根的置换群!

更多的例子

- ① $GL_2(\mathbb{F}_2) \curvearrowright V = \mathbb{F}_2^{\oplus 2}$
- ② $\Sigma(\square) \curvearrowright \text{Vect}(\square)$
- ③ 若 $G \curvearrowright X$, 则 G 自然作用于 $\mathcal{P}(X)$, X 的幂集。

轨道-稳定化子定理

定理

考虑 $G \curvearrowright X$ 以及 $x \in X$ 。则存在双射

$$G/G_x \longrightarrow \mathcal{O}_x, \quad gG_x \mapsto g.x$$

且与 G -作用相容。特别地，我们有轨道-稳定化子公式

$$|\mathcal{O}_x| = |G/G_x| = [G : G_x]!$$

定理 (Cauchy 1845/Frobenius 1887/Burnside 1897)

考虑 $G \curvearrowright X$, 以及轨道集合 G/X 。对于 $g \in G$, 考虑 $X^g = \{x \in X \mid g.x = x\}$ 。则有:

$$|G| \cdot |X/G| = \sum_{g \in G} |X^g|$$

hint: 计数 $\{(g, x) \in G \times X \mid g.x = x\}$!

忠实作用

作用 $G \curvearrowright X$ 的核 $N = \bigcup_{x \in X} G_x$ 。若 $N = 1_G$ ，则 $G \curvearrowright X$ 为忠实的，等价地， $\rho: G \rightarrow S(X)$ 是单同态。

例子

- ① 左正则作用 $G \curvearrowright G$ 是忠实的，故， $G \hookrightarrow S(G)$ (Cayley定理!)
- ② 右正则作用 $G \curvearrowright G$ 定义如下： $g \circ h = hg^{-1}$ ，亦为忠实的。

自由作用

作用 $G \curvearrowright X$ 称为自由的, 若任何 $x \in X$ 满足 $G_x = \{1_G\}$, 等价地, $|\mathcal{O}_x| = |G|$ 。特别地, $|G|$ 整除 $|X|$!

例如: 左右正则作用均为自然作用。

例如: $H \leq G$, 则乘法诱导的作用 $H \curvearrowright G$ 也是自由的。

平凡作用

作用 $G \curvearrowright X$ 称为平凡的, 若 $g.x = x$, 任何 $g \in G$ 以及 $x \in X$, 等价地, $G_x = G$ 。

例子

设 $G \curvearrowright X$ 。则 X 的不动点集 $X^G = \{x \in X \mid g.x = x, \text{ 任何 } g \in G\}$ 。
若 X^G 非空, 则 $G \curvearrowright (X^G)$ 是平凡的。

共轭作用

考虑共轭作用 $G \curvearrowright X = G$ 如下: $g \circ x = gxg^{-1}$

- ① 轨道为共轭类 C_x
- ② $C_x = \{x\}$ 当且仅当 $x \in Z(G)$
- ③ 稳定化子为 $Z(x) = \{g \in G \mid gx = xg\}$, 包含 $\langle x \rangle$
- ④ $|C_x| = \frac{|G|}{|Z(x)|}$

命题 (类等式)

$$|G| = |Z(G)| + \sum_{|C_x| > 1} |C_x|$$

例子

例子

回顾: A_4 的共轭类?

有限群 G 称为 p -群, 若 $|G| = p^n$ 。

命题

p -群均有非平凡中心。

命题

p^2 阶群均为Abel群, 且同构于 $\mathbb{Z}_{p^2}$ 或 $\mathbb{Z}_p \times \mathbb{Z}_p$ 。

例子一

例子

S_4 共轭作用于共轭类

$$X = \{A = (12)(34), B = (13)(24), C = (14)(23)\}$$

考虑相应的群同态

$$S_4 \longrightarrow S(X)$$

例子二

例子

设 $H \leq G$ 。则 G 共轭作用于

$$X_H = \{H' \leq G \mid H' \text{ 共轭于 } H\}$$

则:

$$|G| = |N_G(H)| \cdot |X_H|$$

其中, 正规化子 $N_G(H) = \{g \in G \mid gH = Hg\}$.

命题

设子群 $N \leq G$ 满足 $[G : N] = p$ 为 G 的最小素因子。则 N 为正规子群。

hint: 考虑 $G \curvearrowright G/N$, 其核 K 属于 N 。考虑 $[G : K]!$

近世代数之二十

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① Sylow子群
- ② 例子与应用

Sylow子群

设 $|G| = p^r \cdot m$, 其中 $p \nmid m$ 。

定义

子群 $P \leq G$ 称为**Sylow p -子群**, 若 $|P| = p^r$ 。

定理 (Sylow 1872)

设 $|G| = p^3 \cdot m$ 如上。则下列断言成立:

- ① 存在Sylow p -子群。
- ② Sylow p -子群之间相互共轭; 故, 均同构!
- ③ Sylow p -子群的个数: 是 m 的因子, 其形如 $kp + 1$ 。
- ④ 任何 p -子群 $B \leq G$, 存在Sylow p -子群 P 满足 $B \leq P \leq G$ 。

例子 S_4

例子

- ① $|S_4| = 3^1 \cdot 2^3$
- ② $Sylow$ 2-子群恰有3个! 分别为 $(K_4, (12)), (K_4, (13)), ((K_4, (14)))$
- ③ $Sylow$ 3-子群恰有4个。
- ④ S_4 的4-阶子群不一定相互共轭! 2-阶子群呢?

例子 A_4

例子

- ① $|A_4| = 3^1 \cdot 2^2$
- ② $Sylow\ 2$ -子群仅有一个，为正规子群 K_4 。
- ③ $Sylow\ 3$ -子群有4个。

35阶群

命题

35阶群必同构于 $\mathbb{Z}_{35}$ 。

hint: 考虑Sylow 5-子群 P 以及Sylow 7-子群 Q ; 它们都是正规子群!

108阶群

命题

108阶群总不是单群。

hint: $|G| = 2^2 \cdot 3^3$ 。考虑Sylow 3-子群 P ，考虑 G 左诱导作用于 G/P 。则有同态

$$\rho: G \longrightarrow S(G/P)$$

应用：有限Abel群

命题

设 G 为Abel群，满足 $|G| = p_1^{s_1} \cdots p_r^{s_r}$ 。则其Sylow p_i -子群 P_i 唯一，且有

$$G = P_1 \times P_2 \times \cdots \times P_r.$$

故，归结于Abel p -群结构问题！

应用：最小单群

定理

设 G 为非 $Abel$ 单群。则 $|G| \geq 60$ 。且，60阶单群必同构于 A_5 。

部分证明

- ① 考虑 $X = \{U \leq G \mid |U| = p^r\}$ 。则 $G \curvearrowright X$ 如下 $g.U = gU$ 。
- ② 注意到 $p \nmid |X|$ (试比较 i 以及 $m \cdot p^r - p^r + i$ 的 p -次数)
- ③ 存在 $U \in X$ 使得 $p \nmid |\mathcal{O}_U|$ 。考虑稳定化子 G_U ，
故 $|G_U| = p^r \cdot m'$ 。
- ④ 但, $G_U \curvearrowright U$ freely, 这样 $|G_U|$ 整除 p^r 。故有, $|G_U| = p^r$, 为所求!

近世代数之二十一

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 自由群
- ② 群的表现

字母与字

- ① 考虑集合 X ，添加形式逆 $X^{-1} = \{x^{-1} \mid x \in X\}$
- ② 字母集合 $X \cup X^{-1}$
- ③ 定义字 $w = x_1 x_2 \cdots x_n$, $x_i \in X \cup X^{-1}$
- ④ 既约字：不存在 $x_i = x_{i+1}^{-1}$ ；每个字均能约化为唯一的既约字！
- ⑤ 空字记为1

自由群

定义

集合 X 上的自由群

$$F(X) = \{ \text{所有既约字的全体} \}$$

乘法为字的连接（以及约化）。若 X 为有限集，则 $F(X)$ 称为有限生成自由群。

验证：乘法结合律？

问题：若 $X = \{a\}$ ， $F(X)$ 是什么？

自由群的范性质

命题

设 G 为群以及任何映射 $f: X \rightarrow G$ 。则 f 唯一延拓为群同态 $F(X) \rightarrow G$ 。

命题

任何群均为自由群的商群。

群的表现

定义

群 G 的(有限)表现是指

$$G = \langle x_1, \dots, x_n \mid r_1, r_2, \dots, r_m \rangle, \quad r_i \in F(x_1, \dots, x_n)$$

其中, 右边是指

$$F(x_1, \dots, x_n) / N(r_1, r_2, \dots, r_n)$$

这里, $N(r_1, r_2, \dots, r_m)$ 为包含这些 r_i 的最小正规子群。称 x_i 为生成元, r_i 为生成关系。

问题: 子群 $N(r_1, r_2, \dots, r_m)$ 由哪些元素生成?

命题

设 $G = \langle x_1, \dots, x_n \mid r_1, r_2, \dots, r_m \rangle$ 以及 H 为群。则映射 $f: X = \{x_1, \dots, x_n\} \rightarrow H$ 可延拓至群同态 $G \rightarrow H$ 当且仅当元素 $f(x_i) \in H$ “满足” 关系 r_i 。

The Word Problem (困难!!): G 中的元素? 或, $F(X)/N$ 的陪集代表元系?

记号: $G = \langle x_1, \dots, x_n \mid r_1, r_2, \dots, r_m \rangle$, $r_i \in F(x_1, \dots, x_n)$ 常记为

$$G = \langle x_1, \dots, x_n \mid r_1 = 1, r_2 = 1, \dots, r_m = 1 \rangle$$

例子

例子

证明: $\mu_n \simeq \langle g \mid g^n = 1 \rangle$

例子

证明: $S_3 \simeq \langle s_1, s_2 \mid s_1^2 = 1 = s_2^2, s_1 s_2 s_1 = s_2 s_1 s_2 \rangle$

例子

例子

考虑 $\mathbb{R}^2$ 的正 n 形，其对称群为 D_n ，二面体群，阶为 $2n$ ： n 个旋转以及 n 个发射。

试证明： $D_n \simeq \langle x, y \mid x^n = y^2 = 1, (xy)^2 = 1 \rangle$

表现不唯一： $D_n \simeq \langle s, t \mid s^2 = t^2 = 1, (st)^n = 1 \rangle$.

问题：无限二面体群

$$D_\infty = \langle x, y \mid y^2 = 1 = (xy)^2 \rangle \simeq \langle s, t \mid s^2 = 1 = t^2 \rangle$$

是无限群？

四元数群

例子

考虑四元数代数 $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$, 为可除环。

考虑子群 $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \subseteq \mathbb{H}^\times$ 。

试证明: $Q_8 \simeq \langle a, b \mid a^4 = 1, b^2 = a^2, ba = a^3b \rangle$

问题: Q_8 与 D_4 同构么?

口号: 每个“具体群”都有自己的“故事”!

近世代数之二十二

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 有限生成Abel群
- ② 整数矩阵相抵

加法群

- ① Abel群 A 记为加法群: $a + b$, 么元为 0_A , 负元 $-a$
- ② 两加法群的直积通常记为直和 $A \oplus B = A \times B$
- ③ (有限生成) **自由Abel群** $\mathbb{Z}^n = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$, 其元素通常记为列向量
- ④ $\mathbb{Z}^n$ 有**标准基**; aha, we are doing linear algebra over $\mathbb{Z}$!

自由Abel群

可以定义基

命题

有限生成Abel群 A 是自由的当且仅当 A 有一组基！

子群就是“子空间”！

命题

任何有限生成Abel群均同构于 $\mathbb{Z}^n/K$ ，其中 $K \leq \mathbb{Z}^n$ 为子群。

不平凡的结论！

命题

$\mathbb{Z}^n$ 的任何子群 K 为有限生成的。

提示：对 n 归纳！

矩阵

考虑 $M_{n \times m}(\mathbb{Z})$ 。

命题

存在双射

$$M_{n \times m}(\mathbb{Z}) \longleftrightarrow \{ \text{群同态 } \mathbb{Z}^m \rightarrow \mathbb{Z}^n \}, \quad A \mapsto \phi_A \text{ 左乘矩阵}$$

思考: $\mathbb{Z}^n \simeq \mathbb{Z}^m$ 是否得出 $n = m$?

可定义 ϕ_A 的余核 $\text{Cok}(\phi_A) = \mathbb{Z}^n / \text{Im}(\phi_A)$.

推论

任何有限生成Abel群均同构于 $\text{Cok}(\phi_A)$!

相抵标准型

考虑可逆整方阵的群 $GL_n(\mathbb{Z})$ ，定义相抵。

命题

相抵的矩阵有一样的余核！

定理

设 $A \in M_{n \times m}(\mathbb{Z})$ 。则存在 P, Q 可逆使得

$$P^{-1}AQ = \text{diag}(d_1, d_2, \dots, d_r, 0, \dots, 0)$$

使得正整数 $d_1 | d_2 | \dots | d_r$ 。

推论

推论

考虑方阵 $A \in M_n(\mathbb{Z})$ 。则 $\text{Cok}(\phi_A)$ 有限当且仅当 $\det(A) \neq 0$ 。此时, $|\text{Cok}(\phi_A)| = |\det(A)|$.

推论

考虑 $K \leq \mathbb{Z}^n$ 。则有:

- ① 存在 $\mathbb{Z}^n$ 的一组基 $\{e_1, \dots, e_n\}$, 以及 $d_1 | d_2 | \dots | d_r$, 使得 $\{d_1 e_1, \dots, d_r e_r\}$ 恰为 K 的基。特别地, K 自由!
- ② $\mathbb{Z}^n / K \simeq \mathbb{Z}_{d_1} \oplus \dots \oplus \mathbb{Z}_{d_r} \oplus \mathbb{Z}^{n-r}$.

有限生成Abel群结构定理

Abel 群 G 的扭子群 $t(G) = \{g \in G \mid g \text{ 有限阶}\}$, 是子群!

定理

设 G 为有限生成Abel群。则存在群同构

$$G \simeq \mathbb{Z}^r \oplus t(G),$$

其中 $r = \text{rank}(G)$, 群 G 的秩, $t(G)$ 为有限群, 同构于 $\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}$, d_i 称为 G 的不变因子。

注: 有限 p -群必同构于 $\mathbb{Z}_{p^{s_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{s_t}}$, p^{s_i} 为初等因子。

近世代数之二十三

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① Galois 群
- ② 不变子域
- ③ Galois 扩张

考虑域扩张 K/k , 其Galois群

$$\mathrm{Gal}(K/k) = \mathrm{Aut}(K/k) \leq \mathrm{Aut}(K)$$

引理

设 $\dim_k K < \infty$. 则 $|\mathrm{Gal}(K/k)| \leq \dim_k K!$ 若 $K = (k, f(x))$ 为可分多项式 $f(x) \in k[x]$ 的分裂域, 则等号成立!

想法: 插入中间域 $k(\alpha)$, 考虑可能的延拓!

考虑子群 $G \leq \text{Aut}(K)$, 其不变子群

$$K^G = \{a \in K \mid \sigma(a) = a, \text{ 任何 } \sigma \in G\} \subseteq K$$

这是子域!

- ① $H \leq G$, 则 $K^G \subseteq K^H \subseteq K$
- ② 设 K/k , 且 $G \leq \text{Gal}(K/k)$ 。则 $k \subseteq K^G \subseteq K$
- ③ $k \subseteq K^{\text{Gal}(K/k)}$
- ④ $G \leq \text{Gal}(K/K^G)$

定理

设 $G \leq \text{Aut}(K)$ 为有限子群。则有

- ① $[K : K^G] = |G|$
- ② $G = \text{Gal}(K/K^G)$

证：设 $n = |G|$ 且 $k = K^G$ 。反设 $\{e_1, \dots, e_{n+1}\} \subseteq K$ 是 k -线性无关。考虑 $n \times (n+1)$ 矩阵

$$A = (\sigma(e_1), \dots, \sigma(e_{n+1}))_{\sigma \in G}$$

考虑解空间 $V \subseteq K^{n+1}$ ：它是 G -不变的！

取非零向量 $v = (\lambda_1, \dots, \lambda_{n+1}) \in V$ 使得非零分量最少（非零分量至少两个，且不能都在 k 中！）。

不妨设 $\lambda_1 = 1, \lambda_2 \notin k$ 。取 $g \in G$ 使得 $g(\lambda_2) \neq \lambda_2$ 。

则 $v - g(v) \in V$ ，矛盾！

考虑有限维扩张 K/k , $G = \text{Gal}(K/k)$ 。已知 $k \subseteq K^G$

定理

以下断言等价。

- ① $k = K^G$
- ② $|G| = \dim_k K$
- ③ 任何 $\alpha \in K$, α 的最小多项式无重根, 且在 K 上分裂。
- ④ $K = (k, f(x))$, $f(x) \in k[x]$ 可分多项式。

此时, 称 K/k 为有限 **Galois** 扩张!

定理证明

- ① $(1) \Rightarrow (2)$ 见上定理!
- ② $(2) \Rightarrow (3)$ 回到域同态的延拓!
- ③ $(3) \Rightarrow (4)$ 分裂域的定义
- ④ $(4) \Rightarrow (1)$ 还是回到域同态的延拓(其证明)!

双射

命题

存在双射

$$\{\text{有限子群 } G \leq \text{Aut}(K)\} \longleftrightarrow \{\text{子域 } k \subseteq K \mid K/k \text{ 有限维 Galois}\}$$

命题

设 K/k 为有限维 Galois 扩张。则存在双射

$$\{\text{Gal}(K/k) \text{ 的子群}\} \longleftrightarrow \{K/k \text{ 的中间域}\}$$

注：中间域 E ， K/E 总是 Galois。但，

K/k 是 Galois 的当且仅当 $\sigma(E) = E$ ，任何 $\sigma \in \text{Gal}(K/k)$ 。

例子

- ① $K/\mathbb{F}_p$ 有限域!
- ② $K = (\mathbb{Q}, x^3 - 2)$
- ③ $K = (\mathbb{Q}, (x^2 - 2)(x^2 - 3))$
- ④ 任何有限群 $G \leq S_n$ 作用于 $k(t_1, \dots, t_n)$, 故, 成为Galois群!

近世代数之二十四

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 子群格与子域格
- ② 基本定理

- ① 考虑偏序集 $(L, \leq)$
- ② 最小上界 $\vee$, 最大下界 $\wedge$

定义

偏序集 $(L, \leq)$ 称为格, 若最小上界以及最大下界均存在。

例子

- ① 群 G 的子群格 $\text{Sub}(G)$
- ② 考虑域扩张 K/k 。则中间域的格 $\text{Lat}(K/k)$
- ③ $(L, \leq)$ 的反格

同构

引理

设 L, L' 均为格。设 $f: L \rightarrow L'$ 为偏序集同构。则 f 保持 $\vee$ 以及 $\wedge$ 。

例子

设 $n \geq 1$ 。则 $L_n = \{d \mid 1 \leq d \leq n, d|n\}$ 在整除关系下为格。

设 $C_n = \langle g \mid g^n = 1 \rangle$ 为循环群。则有格同构

$$\text{Sub}(C_n) \longrightarrow L_n$$

Galois理论基本定理

定理

设 K/k 为有限维 *Galois* 扩张, $G = \text{Gal}(K/k)$ 。则有格同构

$$\text{Sub}(G) \longrightarrow \text{Lat}(K/k)$$

$$\text{Gal}(K/K^E) = H \longmapsto K^H$$

在此对应中, 我们有 $\dim_k K^H = [G : H]$ 且 $\dim_{K^H} K = |H|$ 。

回顾: 维数公式 $\Leftrightarrow$ Lagrange 定理!

沿用基本定理。则有

- ① 设 $H, U \leq G$ 。则有

$$K^{H \vee U} = K^H \cap K^U, K^{H \cup U} = K^H \vee K^U.$$

- ② 设 B, E 为中间域。则有

$$\text{Gal}(K/B \vee E) = \text{Gal}(K/B) \cap \text{Gal}(K/E)$$

$$\text{Gal}(K/B \cap E) = \text{Gal}(K/B) \vee \text{Gal}(K/E).$$

推论 (续)

- ① 考虑 $\sigma \in G$ 。则 $\text{Gal}(K/\sigma(E)) = \sigma \text{Gal}(K/E) \sigma^{-1}$
- ② 回顾中间域 E 使得 E/k 是 Galois 扩张 $\Leftrightarrow E$ 在 G 上不变。
- ③ 故，中间域 E 使得 E/k 是 Galois 扩张 $\Leftrightarrow \text{Gal}(K/E) \triangleleft G$ 此时：

$$G/\text{Gal}(K/E) \simeq \text{Gal}(E/k)$$

例子

- ① 考虑 $\mathbb{F}_{p^n}/\mathbb{F}_p$ 的 Galois 对应
- ② 考虑 $K/\mathbb{Q}$, 其中 $K = (\mathbb{Q}, x^3 - 2)$
- ③ 考虑 $K/\mathbb{Q}$, 其中 $K = (\mathbb{Q}, (x^2 - 2)(x^2 - 3))$

引理

考虑 $f(x) = h(x)g(x) \in k[x]$ 。考

虑 $K = (k, f(x))$, $B = (k, h(x))$, $C = (k, g(x))$ 。设 $B \cap C = k$ 。则有

$$\text{Gal}(K/k) \simeq \text{Gal}(B/k) \times \text{Gal}(C/k)$$

提示：考虑正规子群 $\text{Gal}(K/B)$ 以及 $\text{Gal}(K/C)$ ，它们“互补”！

近世代数之二十五

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 本原元定理
- ② 代数基本定理

Steinitz定理

定理 (E. Steinitz 1910)

设 K/k 为有限维扩张。则 K/k 为单扩张当且仅当 K/k 中只有有限个中间域。

注：这与Galois理论无关。

“ $\Rightarrow$ ” 设 $|k| = \infty$ ，考虑 $k(\alpha + t\alpha) \subseteq K = k(\alpha, \beta)$, $t \in k$

“ $\Leftarrow$ ” 考虑生成元 α 在中间域 E 上的最小多项式！

例子

考虑 $k = \mathbb{F}_p(x, y)$ 以及 $K = (k, (t^p - x)(t^p - y))$ 。证明 K/k 有限维，但不是单的。

本原元定理

定理 (E. Galois)

设 K/k 为有限维可分扩张。则 K/k 为单扩张。

考虑 $k \subseteq K \subseteq E$ 使得 E/k 为 Galois 扩张；利用 Galois 对应。

代数基本定理

定理

复数域 $\mathbb{C}$ 是代数封闭的。

注：应该称为“数学基本定理”！

- ① $K/\mathbb{R}$ 。则 $\dim_{\mathbb{R}} K$ 不为奇数。
- ② $K/\mathbb{C}$ 。则 $\dim_{\mathbb{C}} K \neq 2$

证明

- ① 设 $f(x) \in \mathbb{C}[x]$ 不可约。设 $\mathbb{R} \subseteq \mathbb{C} \subseteq K = (\mathbb{C}, f(x))$;
 $G = \text{Gal}(K/\mathbb{R})$
- ② 断言: $|G| = 2^?$ 。(否则, 有子群 H 使得 $[G : H]$ 为奇数、利用 Galois 对应)
- ③ 有 $\dim_{\mathbb{C}} K = 2^{?-1}$ 。考虑 $G' = \text{Gal}(K/\mathbb{C})$ 。它有子群 H 满足 $[G' : H] = 2$ (why?)。再用 Galois 对应!

近世代数之二十六

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① 根式扩张
- ② 可解群

根式扩张

定义

称 E/k 为根式扩张 of type m , 若 $E = k(\alpha)$, 且 $\alpha^m = a \in k$ 。形象地, 我们记 $\alpha = \sqrt[m]{a}$

根式扩张塔是指域扩张的链, 使得相邻的域为根式扩张

$$k = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n$$

注: E_n 从 k 重复“做开根号”得到!

- ① 若 E/k 为根式扩张 of type m , 且 k 包括 m 次本原单位根。则 $E = (k, x^m - a)$ 。此时,

$$\text{Gal}(E/k) \hookrightarrow (\mathbb{Z}_m, +), \quad \sigma \mapsto \bar{i}$$

使得 $\sigma(\alpha) = \alpha\omega^i$ 。

根式可解

定义

多项式 $f(x) \in k[x]$ 称为根式可解, 若存在根式扩张塔

$$k = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n$$

使得 $f(x)$ 在 E_n 上分裂, 即 E_n “包含” $f(x)$ 的分裂域。

例子

考虑 $f(x) = x^2 + bx + c \in \mathbb{C}[x]$ 。则 $k\mathbb{Q}(b, c)$ 为系数域。考虑 $f(x) = (x - r_1)(x - r_2)$ 的分裂域。

则 $k = E_0 \subseteq \mathbb{Q}(r_1, r_2) \subseteq k(\sqrt{b^2 - 4c}) = E_1$ 。

根式扩张塔

- ① 任何根式扩张塔可扩充成新的根式扩张塔，使得 E_n/E_0 是Galois。
- ② 若 $k = E_0$ 有充分多的单位根，则

$$\text{Gal}(E_n/E_0) \supseteq \text{Gal}(E_n/E_1) \supseteq \text{Gal}(E_n/E_2) \supseteq \cdots$$

相邻为正规子群，其因子（商群）为Abel群。

- ③ 一般地，设 k 特征零，我们考虑 $k \supseteq k' = (k, x^m - 1)$ 。则

$$\begin{array}{ccc} k & \hookrightarrow & E_n \\ \downarrow & & \downarrow \\ k' & \hookrightarrow & E'_n \end{array}$$

则 $\text{Gal}(E'_n/k) \supseteq \text{Gal}(E'_n/k')$ ，其商同构于 $\text{Gal}(k'/k)$ ，为Abel群。

可解群

定义

有限群 G 称为可解群, 若存在子群链

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$$

使得 $G_{i+1} \triangleleft G_i$ 且因子 G_i/G_{i+1} 为Abel。

例子

- ① Abel群可解
- ② p 群可解
- ③ 若 G 可解, 则其子群 H 也可解。
- ④ 设 $N \triangleleft G$ 。则 G 可解当且仅当 N 与 G/N 同时可解。
- ⑤ S_n 不可解, $n \geq 5$ 。

方程的Galois群

回顾:

定义

方程 $f(x) \in k[x]$ 的 *Galois* 群

$$\mathrm{Gal}_k(f) = \mathrm{Gal}(E/k),$$

其中 $E = (k, f(x))$ 为其分裂域。

近世代数之二十七

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

- ① Galois大定理
- ② 例子

定理

设 $\text{char } k = 0$ 以及 $f(x) \in k[x]$ 。则方程 $f(x)$ 根式可解当且仅当 $\text{Gal}_k(f)$ 为可解群。

“仅当”的证明

- ① 考虑 $k \subseteq K \subseteq E$ 使得 $K = (k, f(x))$, E/k 为根式扩张塔且为 Galois 扩张。则 $\text{Gal}_k(f)$ 是 $\text{Gal}(E/k)$ 的商。
- ② 考虑 $k' = (k, x^m - 1)$, 适当“大”的 m 。考虑

$$\begin{array}{ccc} k & \hookrightarrow & E \\ \downarrow & & \downarrow \\ k' & \hookrightarrow & E' \end{array}$$

- ③ 从定义, “已知” $\text{Gal}(E'/k')$ 是可解群! 于是, 用可解群的基本事实...

关键引理

引理

设 K/k 为有限维 *Galois* 扩张满足 $\text{Gal}(K/k) = C_p = \langle \sigma \rangle$, p 素数。
设 k 包含 p 次本原单位根。则存在 $\beta \in K$ 使得 $K = k(\beta)$ 且 $\beta^p \in k$ 。

hint: 考虑 k -线性变换 $\sigma: K \rightarrow K$ 关于特征值 ω 的特征向量!

“当”的证明

- ① 设 $K = (k, f(x))$ 以及 $G = \text{Gal}(K/k)$
- ② 若 k 有 $|G|$ 次本原单位根。则 $H \triangleleft G$ 使得 $G/H \simeq C_p$ 。
则 $k \leq K^H \subseteq K$; 归纳即可。
- ③ 添加单位根 $K' = K(\omega)$

$$\begin{array}{ccc} k & \hookrightarrow & K \\ \downarrow & & \downarrow \\ k' & \hookrightarrow & K' \end{array}$$

幸运地是, $\text{Gal}(K'/k') \hookrightarrow G$, 也可解!

例子

例子

考虑 $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$, 它的根 $\{\alpha_1, \dots, \alpha_5\}$, 其中 $\alpha_1 = \overline{\alpha_2}$ 为复根。则 $\text{Gal}_{\mathbb{Q}}(f) = S_5$ 。

注: S_5 可由 (12) 以及任何 5-轮换生成。

例子

例子

考虑 $F = k(t_1, \dots, t_n)$ 为有理函数域。则一般方程定义为：

$$f(x) = x^n - t_1 x^{n+1} + t_2 x^2 + \dots + (-1)^n t_n \in F[x]$$

不可约多项式 (why?), 其 *Galois* 群为 S_n (why?)!

注：考虑 S_n 自然作用于 $k(y_1, \dots, y_n)$, 研究其不变子域 (有限群的不变量理论!)。