抽象代数笔记
域与域扩张

EndlieDownAHell

2023 年 8 月 29 日

概览

这一节便是所谓经典抽象代数学的顶点: Galois 理论, 更具体说, 则是域扩张与群的一系列对应, 也即通过域的自同构生成的 Galois 群, 其根源在于方程根的置换, 这是 Galois 群的最早形态, 也即解的置换群, 而后再改为分裂域的自同构群, 也即是域扩张的自同构群. 这些理论的现代面貌由 Artin 改造而出.

§7.1 给出了域扩张下 Galois 群的概念, 也从反方向给出了自同构群的定域的概念. 这一番穿梭在 §7.2 中发展为了更严谨的 Galois 扩张下的闭域与闭子群的对应, 这对应也是中间域等价与子群共轭的对应, 总而言之, 这一节实际上是探明了我们所需的 Galois 群与中间域自由穿梭所需的良好性质, 也即 Galois 扩张 (正规可离扩张).

§7.3 通过多项式的分裂域将 Galois 群配置到了多项式上, 并探讨了一系列特殊多项式的 Galois 群, 这为 §7. 4,5 关于多项式根号可解性的探讨打下了基础, 其中光辉灿烂的结果便是所谓的可解多项式与可解群的关系, 最后的 §7.5 则是 Galois 理论在尺规作图问题上的一些简单应用.

逐节评注

§7.1 Galois 群

这一节给出了 Galois 群的定义, 并讨论了一些具体例子, 其中超越扩张 $F(x)$ 的 Galois 群同构于 $\mathrm{GL}_2(F)/\{\mathrm{diag}(a,a) \mid a \in F\}$ 是很有意思的结果.

之后本节又尝试从自同构群中给出相应的子域使得这自同构群为一 Galois 群, 与前文结合后我们得到了 Galois 群与相应的域扩张的基本联系的定理, 也即定理 7.1.2, 本节最终以正规底定理收尾.

Expansion 1 补充下定义 7.1.1 缺失的证明

命题 1 取定 E 为 F 的子域, 使得 E 不动的全体 F 的自同构构成一个群 G.

Proof. 依照复合定义运算, 则结合律自动成立, 对于 $\sigma_1, \sigma_2 \in G$, 从下式即得封闭性成立:

$$\forall x \in E, \sigma_1 \circ \sigma_2(x) = \sigma_1(x) = x$$

取定 id_F, 我们再来证明幺元与逆元的存在,

$$\sigma \circ \mathrm{id}_F = \sigma = \mathrm{id}_F \circ \sigma$$

由于 G 的成员是自同构, 所需的逆元自动存在. □

Explanation 1 定理 7.1.1 的证明思路大致如下:

考虑到 E 关于 F 的 Galois 群, G 就在其中, 且其内部的每一个 F 自同构实际上对应着 F 的一个互异等价, 而后者不大于 $(F:E)$, 假如能够额外证明 G 的阶数大于 $(F:E)$, 即能说明 G 就是那个 Galois 群.

为此我们需要说明 E 作为 F 上的线性空间至多是 n 维的, 证明这件事只需要找到 E 中 $n+1$ 个线性相关的向量, 这便是证明中所作构造的目的, 顺带原书证明不明不白之处颇多, 请再仿看 §7.2 Explanation 3.

§7.2 域与群的结对关系

这一小节主要建立的是 Galois 扩张与 Galois 群之间的关系, 推论 7.2.1 之前的工作说明了 $L \to L', G \to G'$ 的众多缺陷, 建立了这一对应关系下的一些包含关系与不等式, 定理 7.2.3 则通过限制了可分与正规这两个属性, 得到了等式成立所需的 Galois 扩张, 之后的几条命题便是相关性质的摹写了.

Explanation 2 命题 7.2.1 的证明大要如下:

采取归纳法的思路, 我们很容易解决存在中间域的情形, 当中间域不存在时, 这扩张便是单纯扩张, 此时考虑自同构里代数元 u 将被指向的对象, 自然只能是 u 的共轭根.

另一方面, 由于 M' 本身的成员是不变动 u 的, 于是, 商群 L'/M' 中各代表元 $l'+M'$ 只靠 $l'(u)$ 为何物区分, 自然 $|L'/M'|$ 不大于 u 的极小多项式的次数, 进而不大于 n.

Explanation 3 我们来补完命题 7.2.2 的证明.

命题 2 取定 G 是域 E 关于 F 的 Galois 群, 且有 $J < H < G$, 若 $(J:H) = n$, $(H':J') \leq n$.

Proof. 取定 H' 中的 $n+1$ 个元素 $\mathfrak{h}_1, \cdots, \mathfrak{h}_{n+1}$, 生成一列向量:

$$\varepsilon_{\mathfrak{i}} = (j_1(\mathfrak{h}_{\mathfrak{i}}), \cdots, j_n(\mathfrak{h}_{\mathfrak{i}})), \mathfrak{i} = 1, \cdots, n+1$$

其中 $j_1, \cdots, j_n$ 是 J/H 的 n 个代表元, 自然 $\{\varepsilon_{n+1}\}$ 在 H'^n 线性相关, 取其一个极大线性无关组 $\varepsilon_1, \cdots, \varepsilon_r$, 对于 ε_{r+1} 即得表出 $\varepsilon_{r+1} = \sum_{k=1}^{r} \mathfrak{h}_k \varepsilon_k, \mathfrak{h}_k \in H'$, 分拆开来也就是

$$j_t(\mathfrak{h}_{r+1}) = \sum_{k=1}^{r} \mathfrak{h}_k j_t(\mathfrak{h}_k), t = 1, \cdots, n$$

追加 j_l 作用之, 得到 $j_l j_t(\mathfrak{h}_{r+1}) = \sum_{k=1}^{r} j_l(\mathfrak{h}_k) j_l j_t(\mathfrak{h}_k)$, 由于 $j_l j_t$ 遍历 G 中成员, 调换顺序即得

$$\sum_{k=1}^{r} [\mathfrak{h}_k - j_l(\mathfrak{h}_k)] \varepsilon_k = 0, l = 1, \cdots, n$$

由于 $\varepsilon_1, \cdots, \varepsilon_r$ 线性无关, 只能是 $j_l(\mathfrak{h}_k) = \mathfrak{h}_k$, 则 $\mathfrak{h}_1, \cdots, \mathfrak{h}_r \in J'$, 将其改写为 $\mathfrak{j}_1, \cdots, \mathfrak{j}_r$ 的形式, 前式还可写为

$$j_t(\mathfrak{h}_{r+1}) = \sum_{k=1}^{r} \mathfrak{j}_k j_t(\mathfrak{h}_k)$$

取 j_t 为恒等元, 所需的线性相关便是成立的. □

Explanation 4 定理 7.2.3 上边那堆论述属实一坨, 重证明如下:

命题 3 取定 Galois 扩张[1]E/F, 取定其中的中间域 $E > L > F$, 则 $L'' = L$.

Proof. 非如此, 取定 $u \in L'' - L$, 则 u 在 L 上的极小多项式应当是二次以上的, 考虑到扩张 E/F 是代数且可分的, 则存在 $\mathfrak{u}$ 与 u 共轭, 进而得到 L 不变的同构 $L(u) \simeq L(\mathfrak{u})$, 这同构立马可以开拓为 E 的自同构, 这同构自然在 L' 里, 却使得 u 变动, 这是矛盾的, 于是只能 $L = L''$. □

Explanation 5 对定理 7.2.4 的证明, 我们只补充两个被省略的式子:

$$\sigma \circ \sigma' \circ \sigma^{-1}[\sigma(\alpha_1)] = \sigma \circ \sigma'(\alpha_1) = \sigma(\alpha_1), \sigma' \in L_1'$$

于是 $\sigma(\alpha_1)$ 在 $\sigma L_1' \sigma^{-1}$ 的定域中.

$$\sigma^{-1} \circ \sigma' \circ \sigma[\sigma^{-1} \circ \sigma(\alpha_1)] = \sigma^{-1} \circ \sigma'[\sigma(\alpha_1)] = \sigma^{-1} \circ \sigma(\alpha_1), \sigma' \in L_2'$$

于是 $\sigma^{-1} L_2' \sigma$ 的成员使得 $\alpha_1 = \sigma^{-1} \circ \sigma(\alpha_1)$ 不变.

§7.3 多项式的 Galois 群

这一节通过多项式的分裂域的 Galois 群导出了多项式的 Galois 群, 后者实际上也便是多项式解的置换群的子群. 之后, 本节讨论了几个实例, 在讨论单根号扩张上得出了单根号扩张与循环扩张的关系. 讨论 p 次扩张的过程中, 多项式 $x^p - x - p$ 发挥了重要的作用. 最后本节通过判别式 Δ 讨论了三次及四次多项式的 Galois 群.

Explanation 6 命题 7.3.1 实际上在说, 假若域 F 已经配备了全体 n 次单位方根, 因式分解 $x^n - a$ 只需再添加 a 的 r 次方根, 其中 $r \mid n$.

Explanation 7 防止有和我一样的铸币没反应过来, 对定理 7.3.3 进行补充:

命题 4 取定 β 为 b 的 n 次根, 若 $[F(\beta) : F] = n$, 则 $x^n - b$ 在 F 上既约.

Proof. 若既约, 则 β 的最小多项式次数小于 n, 进而 $[F(\beta) : F] < n$, 矛盾. □

Explanation 8 对命题 7.3.2 我们进行如下重述:

命题 5 符号与假设同 7.3.2, 则 E 关于 F 的 Galois 群的阶为 p.

Proof. 假定 $\sigma(b) = b + k$, 则我们立即有

$$\sigma(b + l) = \sigma(b) + \sigma(l) = b + k + l$$

于是 σ 完全可由 $\sigma(b)$ 决定, 后者具有 p 种不同的可能, 于是 σ 共有 p 种, 相应的 Galois 群的阶数便为 p. □

[1]不知道的请自行百度

§7.4, 7.5 解多项式

§7.4 节给出了 Galois 理论的第一个辉煌应用, 即多项式可用根号解出的充分必要条件. 大致路径十分简单, 先将开根号的行为通过根号扩张加入到解多项式的过程中, 进而再通过循环扩张与 Abel 塔加细为循环塔完成双向命题的证明.

§7.5 节旨在通过一般多项式给出五次以上不可根式解方程的例子, 具体而言则是构造出了 Galois 群确为 S_n 的方程, 之后的例 7.5.1 则是很经典的解三, 四次方程的过程.

Expansion 2 我们解决定理 7.4.1 证明中的一个遗留问题, 具体陈述如下:

命题 6 可解群的子群与商群也是可解群.

Proof. 对于可解群 G, 我们有如下自然的 Abel 塔宣称其可解性:

$$G_0 \rhd G_1 \rhd \cdots \rhd G_n \rhd \{e\}$$

其中 $G_0 = G, G_{i+1} = [G_i, G_i]$. 同样的, 假如如上所言的 Abel 塔存在, 群 G 自然也是可解群.

现在, 对于可解群 G, 采取上文中的符号, 对于其子群 H, 由于恒成立 $H_i < G_i$, 则总将成立 $H_n = \{e\}$ 对某个 n 成立, 进而其是可解的.

另外的, 考虑商群 G/H, 我们先来证明几个引理:

考虑式子 $g_c[h_1, h_2]g_c^{-1}$ 其中 $g_c = [g_1, g_2]$, 我们不难将其改写为 $[g_ch_1g_c^{-1}, g_ch_2g_c^{-1}]$, 考虑到 $H \lhd G$, 则 $g_ch_ig_c^{-1} \in H, i = 1, 2$, 从而得到

$$[g_1, g_2][h_1, h_2][g_1, g_2]^{-1} = [g_ch_1g_c^{-1}, g_ch_2g_c^{-1}] \in [H, H]$$

于是知道 $[G, G] \rhd [H, H]$, 另外的, 建立对应

$$[G/H, G/H] \to [G, G]/[H, H], [g_1H, g_2H] \to [g_1, g_2][H, H]$$

不难将这对应开拓为同构, 于是我们确知了 $[G/H, G/H] \simeq [G, G]/[H, H]$, 再进一步还有

$$[(G/H)_1, (G/H)_1] \simeq [G_1/H_1, G_1/H_1] \simeq [G_1, G_1]/[H_1, H_1] \simeq G_2/H_2$$

以此类推我们立即将要断言 $(G/H)_n = G_n/H_n$, 考虑到对充分大的 n 将成立 $G_n = \{e\}, H_n = \{e\}$, 于是我们能够建立 G/H 的一座以 $\{e\}$ 收尾的交换塔, 从而确定 G/H 是可解的. □

Expansion 3 我们来将说不通一点的定理 7.5.1 证明进行一个重述:

考虑一般多项式的展开形式

$$f(x) = \prod_{k=1}^{n}(x - t_k)$$

则对于另一个表出 $f(x) = \sum_{k=0}^{n}(-1)^{n-k}u_kx^k$, 我们知道诸 u_i 是 t_i 的对称多项式. 则不难发现, 诸多 $F(t_1, \cdots, t_n)$ 的自同构里, 使得 $F(u_1, \cdots, u_n)$ 不变 (再细致一些是诸 u_i 不变) 是且仅是 $\{t_1, \cdots, t_n\}$ 的置换.

于是, $F(U)[x]$ 上的多项式 $f(x)$ 的分裂域 $F(T)$ 所具有的 Galosi 群 (保证 $F(U)$ 不变的 $F(T)$ 的自同构) 便是 T 上的置换, 也即 S_n.

§7.6 尺规作图

这一节没有太大实质性困难, 除了作者还是偶尔抽风不说人话, 大致的脉络是先说明了尺规作图只能对域进行二次扩张, 相应的, 能被尺规作图的点只能是域反复二次扩张有限次的结果, 借此我们能够解决尺规作图的三大难题:

(i) 化圆为方: 由于 π 是超越元, 无法通过尺规作图从 $\mathbb{Q}$ 中得到 $\sqrt{\pi}$, 则化圆为方不可能.

(ii) 立方倍积: 由于 x^3-2 在 $\mathbb{Q}$ 的分裂域是 $\mathbb{Q}$ 三次扩域, 无法通过尺规作图得到 $\sqrt[3]{2}$, 则立方倍积不可能.

(iii) 三等分角: 考虑 60° 的特殊情形, 则 $\cos 20^\circ$ 与方程 $x^3-3x-1=0$ 相关, 多项式 x^3-3x-1 在 $\mathbb{Q}$ 上是既约的, 于是不能通过二次扩张解出, 则三等分角不总可能.

另外的, 借助一点数论的工具, 这一节还得出了正 n 边形可尺规作图的充分必要条件.