Galois 理论——代数数论专题 I

August 25, 2020

0、前言

这是一份介绍 Galois 理论的讲义，内容相较于中规中矩的教材来说是要多得多的，即使这份讲义看上去很简短.

现代代数数论的敲门砖之一就是 Galois 理论，虽然这部分数论都不如代数数论的其他部分来的花哨，但作为基础知识来说它却尤为重要. 现今本科的通识教育连扫盲都做不到，这导致国内绝大部分本科生甚至研究生连域扩张都没听说过，即使他们的抽象代数课程仍取得了不错的成绩. 本来这份讲义将要作为我在南京信息工程大学代数数论系列讨论班上的讲稿，但是因为没人来听，忙于考研，计划便不幸夭折.

在解二次、三次有理系数方程时我们能够感觉到它们的根之间存在某种对称性，只不过这里的对称性在较小的域上被隐藏起来了 (例如在实数上来看没有办法区分出共轭的复数)，而探测这种对称性的办法就是通过一步一步的域扩张 (Galois 扩张)——在更大的域上通过某种特殊自同构的手段来寻找这些根之间对称性的信息 (Galois 对应，定理 51). 例如要想区分方程 $x^2+1=0$ 的根 $\pm\mathrm{i}$，我们就得在域 $\mathbb{C}$ 上来看：$\pm\mathrm{i}$ 可被两种不同的自同构 $\mathbb{C}\to\mathbb{C}, z\mapsto z, z\mapsto\bar{z}$ 区别. 这种思路的抽象化就是 Galois 理论的来源.

本讲义从简单的域扩张开始，依次介绍多项式理论、Galois 基本定理、Galois 理论的应用、无穷 Galois 扩张、超越扩张等. 阅读这份讲义的预备知识就是初步的抽象代数，到后半部分还会需要一些拓扑和其它的代数工具 (可惜我不愿意花力气再写这些东西了，因为它们已经偏离 Galois 理论的范畴).

参考文献

[1] J.S. Milne. Fields and Galois Theory.(J.S. Milne 的主页：https://www.jmilne.org/math/index.html)

[2] P. Morandi. Field and Galois Theory(GTM167). Springer.

[3] 聂灵沼，丁石孙. 代数学引论 (第二版). 高等教育出版社.

[4] O. Forster. Lectures on Riemann Surfaces(GTM81). Springer-Verlag.

[5] 周哲. 伽罗瓦理论 (六). 妈咪说 MommyTalk(Bilibili-AV45347632).

[6] 维基百科：Picard–Vessiot theory.(Michael F. Singer 的主页：https://singer.math.ncsu.edu/index.html)

[7] Henryk Żołçdek. The Monodromy Group. Birkhäuser Verlag.

[8] A. Khovanskii. Topological Galois Theory. Springer.

[9] T. Crespo, Z. Hajto, E.S.-Adamus. Galois Correspondence Theorem for Picard-Vessiot Extensions. Arnold Math J. (2016) 2:21–27. DOI 10.1007/s40598-015-0029-z.

[10] 王杰. 典型群引论. 北京大学出版社.

[11] A. Khovanskii. Galois Theory, Coverings, and Riemann Surfaces. Springer.

[12] J.J. Rotman. An Introduction to Homological Algebra. Springer.(范畴论：https://ncatlab.org/nlab/show)

[13] J. Neukirch. Algebraic Number Theory. Springer.

[14] P.A. Grillet. Abstract Algebra(GTM242). Springer.

[15] F. Diamond, J. Shurman. A First Course in Modular Forms(GTM228). Springer.

朱子阳[1]，2020 年 1 月于重庆理工大学

[1]邮箱 zhuziyang98@163.com

1、预备知识

定义 1(特征) 设 F 是域，可以验证 $\varphi:\mathbb{Z}\to F, n\mapsto n\cdot 1_F=1_F+\cdots+1_F(n\text{ 个})$ 是一个环同态，因此 $\ker\varphi$ 是 $\mathbb{Z}$ 的理想.

(1) 若 $\ker\varphi=(0)$，即 $n\cdot 1_F=0$ 可推出 $n=0$，也就是说任一非零整数被 φ 映为 F 的可逆元. 此时有单同态 $\mathbb{Q}\hookrightarrow F, m/n\mapsto(m\cdot 1_F)(n\cdot 1_F)^{-1}$，即 $\mathbb{Q}\subseteq F$. 称这里域 F 的**特征**为 0，记为 $\mathrm{Char}(F)=0$；

(2) 若 $\ker\varphi=(p)$，p 是素数 (如果 p 不是素数，则 $p=p_1p_2$，因此 $\varphi(p)=\varphi(p_1)\varphi(p_2)=(p_1\cdot 1_F)(p_2\cdot 1_F)=0$，与 F 无零因子矛盾). 此时 φ 诱导单同态 $\mathbb{Z}/p\mathbb{Z}\hookrightarrow F,[n]\mapsto n\cdot 1_F$. 若记 $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$，则 $\mathbb{F}_p\subseteq F$. 称这里域 F 的特征为 p，记为 $\mathrm{Char}(F)=p$.

$\mathbb{Q}$、$\mathbb{F}_p(p$ 是素数) 称为**素域**. 任一个域 F 能且只能包含一种素域 (即 $\mathbb{Q}$、$\mathbb{F}_p$ 中的某一个). 因此 $|F|=\infty$(此时 F 的特征可为 0 也可不为 0，见命题 35) 或 $|F|=p^n(p$ 是素数，$n\geq 1$. 此时 F 的特征为 $p)$.

注意 由于在任意交换环上有二项式定理

$$(a+b)^m=a^m+\binom{m}{1}a^{m-1}b+\cdots+b^m,$$

因此在特征为 p 的域 F 上，由于 $p|\binom{p^n}{k}, k=1,\cdots,p^n-1$，故 $(a+b)^{p^n}=a^{p^n}+b^{p^n}$ 对任意 $n\geq 1$ 均成立. 此时可定义特征为 p 的域 F 上的 **Frobenius 自同态**$F\to F, x\mapsto x^p$. 若又有 $|F|<\infty$，则此自同态是自同构.

例 取 $F=\mathbb{F}_p$，由 Femart 小定理，$[n^{p-1}]=[1]$，因此 Frobenius 自同态即同构 $F\xrightarrow{\sim}F,[n]\mapsto[n]^p=[n]$.

命题 2 设 F 是域，则有一一对应：

$$\begin{aligned}\{F[x]\text{非零理想}\}&\longleftrightarrow\{F[x]\text{中首一多项式}\}\\ I&\longrightarrow I\text{中次数最低的首一多项式}\varphi\\ \big(f(x)\big)&\longleftarrow f(x).\end{aligned}$$

证明思路 对任意 $f\in I$，$f=q\varphi+r$，其中 $\deg(r)<\deg(\varphi)$，则 $r=f-q\varphi\in I$ 与 φ 的次数最低性矛盾.■

作为铺垫，下面给出几个判断 $\mathbb{Q}$ 上多项式是否可约的办法，这一部分常见于各种高等代数教材.

命题 3 设 $r=\alpha/\beta\in\mathbb{Q},\alpha,\beta\in\mathbb{Z},(\alpha,\beta)=1$. 若 r 是多项式 $a_mx^m+a_{m-1}x^{m-1}+\cdots+a_0(a_i\in\mathbb{Z})$ 的根，那么 $\alpha|a_0,\beta|a_m$.

命题 4(Gauss) 设 $f\in\mathbb{Z}[x]$，若 $f=pq(p,q\in\mathbb{Q}[x]$ 且不为常数)，则存在 $p_1,q_1\in\mathbb{Z}[x]$ 使得 $f=p_1q_1$.

推论 5 若 $f\in\mathbb{Z}[x]$ 首一，则 f 的在 $\mathbb{Q}[x]$ 中的任意首一因式亦在 $\mathbb{Z}[x]$ 中.

定义 6(代数整数) 设 $\alpha\in\mathbb{C}.\alpha$ 称为一个**代数整数**，如果它是 $\mathbb{Z}[x]$ 中某个首一多项式的根.

例 根据命题 3，任意 $\mathbb{Q}$ 中的代数整数都属于 $\mathbb{Z}$.

命题 7(Eisenstein) 设 $f=a_mx^m+a_{m-1}x^{m-1}+\cdots+a_0\in\mathbb{Z}[x]$，若存在素数 p 满足：

$(1)p\nmid a_m$；$(2)p|a_{m-1},p|a_{m-2},\cdots,p|a_0$；$(3)p^2\nmid a_0$，则 f 在 $\mathbb{Q}[x]$ 中不可约.

注意 命题 4、推论 5、命题 7 中，将 $\mathbb{Z}$ 换成任一 UFD、$\mathbb{Q}$ 换成其分式域之后这些命题仍然成立.

命题 8 设 $f=a_mx^m+a_{m-1}x^{m-1}+\cdots+a_0\in\mathbb{Z}[x]$. 若存在素数 p，$p\nmid a_m$，且 $f(\mathrm{mod}\ p)$ 在 $\mathbb{F}_p[x]$ 中不可约，则 f 在 $\mathbb{Z}[x]$ 中不可约.

证明思路 若 $f=gh$，$g,h\in\mathbb{Z}[x]$，模 p 得 $\bar f,\bar g,\bar h\in\mathbb{F}_p[x]$ 且 $\bar f=\bar g\bar h$.■

例 由命题 3，x^4-10x^2+1 在 $\mathbb{Z}[x]$ 中不可约，但模 2 之后在 $\mathbb{F}_2[x]$ 中可约：$x^4+[1]=(x^2+[1])^2$. 因此命题 8 的逆命题为假.

定义 9(域扩张) 记 $F\subseteq E$ 都是域，则称 E 是 F 的一个**域扩张**，记为 E/F. 易见 E 是 F-线性空间，其维数 $\dim_F(E)$ 称为扩张的**次数**，记为 $[E:F]$. 若 $[E:F]<\infty$，则称 E/F 为**有限扩张**. 设 E、E' 均是 F 的域扩张，环同态 $\varphi:E\to E'$ 称为一个 F**- 同态**，如果 $\varphi|_F=\mathrm{id}_F$.

例 $\mathbb{C}/\mathbb{R}$ 是次数为 2 的域扩张；$\mathbb{R}/\mathbb{Q}$ 是次数为 ∞ 的域扩张.

命题 10 设有域 $F\subseteq E\subseteq L$，则 $[L:F]<\infty$ 当且仅当 $[L:E]<\infty$ 且 $[E:F]<\infty$. 此时有计算公式

$[L:F]=[L:E][E:F]$.

证明思路 设 $\dim_E(L)=m$. 对任意 $x\in L$，$x=\sum_{i=1}^m x_ie_i$，其中 $x_i\in E,e_i\in L$. 又设 $\dim_F(E)=n$，则 $x_i=\sum_{j=1}^n y_{ij}\eta_j$，其中 $y_{ij}\in F,\eta_j\in E$. 因此 $x=\sum_{i=1}^m(\sum_{j=1}^n y_{ij}\eta_j)e_i$，此时 $\{\eta_je_i|j=1,\cdots,n;i=1,\cdots,m\}$ 是基.■

定义 11(生成) 容易证明：子环 (域) 的交仍是子环 (域).

(1) 设 F 是域 E 的子域，S 是 E 的一个子集. 记 E 中由 F 及 S 生成的子环 $\bigcap\{R|F,S\subseteq R\subseteq E,R是E的子环\}$ 为 $F[S]$. 若 $S=\{\alpha_1,\cdots,\alpha_n\}$，则 $F[S]$ 又可记为 $F[\alpha_1,\cdots,\alpha_n]$. 例如 $\mathbb{C}=\mathbb{R}[\mathrm{i}]$.

(2) 设 F 是域 E 的子域，S 是 E 的一个子集. 记 E 中由 F 及 S 生成的子域 $\bigcap\{L|F,S\subseteq L\subseteq E,L是E的子域\}$ 为 $F(S)$. 若 $S=\{\alpha_1,\cdots,\alpha_n\}$，则 $F(S)$ 又可记为 $F(\alpha_1,\cdots,\alpha_n)$. 例如 $\mathbb{C}=\mathbb{R}(\mathrm{i})=\mathbb{R}[\mathrm{i}]$.

注意 $F[S]$ 显然是整环. 若 $F[S]$ 是域，则 $F(S)\cong F[S]$. 上面 $\mathbb{R}(\mathrm{i})=\mathbb{R}[\mathrm{i}]$ 就是一个例子. 当然，这也是下述命题中 (2) 的一个推论：

命题 12 $(1)F[S]=\{\sum^{<\infty}a_{i_1\cdots i_n}\alpha_1^{i_1}\cdots\alpha_n^{i_n}|a_{i_1\cdots i_n}\in F,\alpha_i\in S,i_j\in\mathbb{N}\}$. 它是包含 F 及 S 最小的 E 的子环.

$(2)F(S)=\mathrm{frac}(F[S])$. 它是包含 F 及 S 最小的 E 的子域.

例 $\mathbb{Q}[\pi]=\{a_m\pi^m+\cdots+a_0|a_i\in\mathbb{Q}\},\mathbb{Q}(\pi)=\{f/g|f,g\in\mathbb{Q}[\pi],g\neq0\}$.

定义 13(单扩张) 一个域扩张 E/F 称为**单扩张**，如果存在 $\alpha\in E$，使 $E=F(\alpha)$. 例如 $\mathbb{Q}(\mathrm{i}),\mathbb{Q}(\pi)$ 就是 $\mathbb{Q}$ 的单扩张.

定义 14(复合域) 设 F,F' 是域 E 的子域，则 F 与 F' 的**复合域**定义为 $F(F')$ 或 $F'(F)$，记作 $F\cdot F'$.

一个很自然的问题：对于域扩张 E/F，该如何描述 E 的结构？我们将分为两种情况：超越扩张 (Case1) 与代数扩张 (Case2) 来讨论. 容易发现，任给 $\alpha\in E$，有很自然的环同态 $\tau:F[x]\to E,f(x)\mapsto f(\alpha)$.

Case1：$\ker\tau=(0)$. 因此 $f(\alpha)=0$ 可以推出 $f\equiv0\in F[x]$，即 α 不是任一非零多项式的根. 此时称 α 是 F 上的**超越元**. 在这个情况下，有环同构 $F[\alpha]\xrightarrow{\sim}F[x](x$ 是未定元$),\alpha\mapsto x$. 取分式域，则得到域同构 $F(\alpha)\cong\mathrm{frac}(F[x])\cong F(x)$. 这时 $F(\alpha)/F$ 是一个“超越扩张”. 一般地，如果域扩张 E/F 中 E 含有 F 上的 (一个) 超越元，就称 E/F 为**超越扩张**. 易见超越扩张的次数为 ∞.

例 $\sum\limits_n\frac{1}{a^{n!}},a\geq2$ 在 $\mathbb{Q}$ 上超越.

Case2：$\ker\tau\neq(0)$. 所以存在非零多项式 $g\in F[x]$ 使 $g(\alpha)=0$. 此时称 α 是 F 上的**代数元**.$\ker\tau$ 的首一生成元 f 称为 α 在 F 上的**极小多项式** (见命题 2). 显然极小多项式一定是不可约的. 下面的命题给出了极小多项式的判定方法：

命题 15 f 是 α 在 F 上的极小多项式，如果满足下述条件之一：

$(1)f$ 首一，$f(\alpha)=0$，且若 $g\in F[x],g(\alpha)=0$，则有 $f|g$；

$(2)f$ 是使 $f(\alpha)=0$ 的次数最低的首一多项式；

$(3)f$ 首一，不可约，且 $f(\alpha)=0$.(因此极小多项式和不可约多项式之间的区别在于是否“首一”)

Case2 中的域扩张 $F(\alpha)/F$ 是一个“代数扩张”. 一般地，如果域扩张 E/F 中 E 的所有元素在 F 上代数，则称 E/F 为**代数扩张**.

注意到极小多项式都是首一不可约的，因此我们有如下重要的命题：

命题 16(代数扩张的结构) 设 $f\in F[x]$ 为 m 次首一不可约多项式，则 $F[x]/(f)$ 为 F 的一个代数扩张，且扩张次数为 m. 若设 α 是 f 的任一个根，即 $f(\alpha)=0$，那么有域同构 $F[\alpha]\xrightarrow{\sim}F[x]/(f),\alpha\mapsto x+(f)$.

注意 命题 16 中，由于 $F[\alpha]$ 已经是域，故 $F(\alpha)=F[\alpha]$. 此后在命题 16(代数扩张) 的前提下，圆括号或方括号可以不加区分. 但是在超越扩张中，圆括号和方括号区别还是很大的.

例 (1) 设不可约多项式 $f=x^2+1\in\mathbb{R}[x]$，则 $\mathbb{R}[x]/(f)\cong\mathbb{R}[\mathrm{i}]\cong\mathbb{C}$. 此时 $[\mathbb{C}:\mathbb{R}]=2$.

(2) 设不可约多项式 $f=x^3-2\in\mathbb{Q}[x]$，我们已经可以计算出 f 的根为：$\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2$，其中 $\omega=\mathrm{e}^{\frac{2\pi}{3}\mathrm{i}}$. 设 $\alpha\in\{\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2\}$，由命题 16 知 $\mathbb{Q}[x]/(x^3-2)$ 为 $\mathbb{Q}$ 的 3 次扩张，且有 $\mathbb{Q}[x]/(x^3-2)\cong\mathbb{Q}[\alpha]\cong\mathbb{Q}[\sqrt[3]{2}]\cong\mathbb{Q}[\sqrt[3]{2}\omega]\cong\mathbb{Q}[\sqrt[3]{2}\omega^2]$. 特别地，$\mathbb{Q}[\alpha]$ 作为 $\mathbb{Q}$-线性空间的基是 $\{1,\alpha,\alpha^2\}$. 注意，这里 $\sqrt[3]{2}$ 与 ω 是“捆绑”在一起的，没有办法区分出 $\sqrt[3]{2}$ 与 ω. 若要想区分它们，则需要一个“更大”的域扩张：$\mathbb{Q}[\sqrt[3]{2},\mathrm{i}]/\mathbb{Q}$. 它作为 $\mathbb{Q}$-线性空间的基是 $\{1,\sqrt[3]{2},\mathrm{i},\sqrt[3]{2}^2,\sqrt[3]{2}\mathrm{i},\sqrt[3]{2}^2\mathrm{i}\}$，即 $[\mathbb{Q}[\sqrt[3]{2},\mathrm{i}]:\mathbb{Q}]=6$.

注意 在命题 16 中，既然 $F[x]/(f)$ 是一个域，自然要问 $\bar{g}\in F[x]/(f)$ 的逆元是什么. 为此我们提供一个

算法. 规定 $f\nmid g\in F[x]$，否则 $\bar{g}=0$. 由于 f 不可约，所以 $(f,g)=1$，因此存在 $u,v\in F[x]$，使 $uf+vg=1$，即 $\bar{v}\bar{g}=\bar{1}$. 故 $(\bar{g})^{-1}=\bar{v}$. 这里的 u,v 可以通过带余除法找到.

命题 17 设 $F(\alpha)/F$ 是单扩张，Ω/F 是一个域扩张. 又设 $\varphi_0:F\to\Omega$ 是一个同态，则：

(0)φ_0 要么是零同态，要么是嵌入 (此时 $\varphi_0(F)$ 是域).

(1) 设 α 在 F 上超越，则对任意 F-同态 (即 $\varphi_0=\mathrm{id}_F$ 的情况) $\varphi:F(\alpha)\to\Omega$，$\varphi(\alpha)$ 仍在 F 上超越. 一般地，有更为广泛的一一对应：

$$\begin{aligned}\{\text{同态}F(\alpha)\xrightarrow{\varphi}\Omega\text{满足}\varphi|_F=\varphi_0\}&\longleftrightarrow\{\Omega\text{中在}\varphi_0(F)\text{上的超越元}\}\\ \varphi&\longrightarrow\varphi(\alpha)\\ \big(\varphi:\alpha\mapsto x;\beta\mapsto\varphi_0(\beta),\beta\in F\big)&\longleftarrow x.\end{aligned}$$

(2) 设 α 在 F 上代数，其极小多项式为 $f(x)$，则对任意 F- 同态 (即 $\varphi_0=\mathrm{id}_F$ 的情况) $\varphi:F[\alpha]\to\Omega$，$\varphi(\alpha)$ 仍是 $f(x)$ 在 Ω 中的根. 一般地，有更为广泛的一一对应：

$$\begin{aligned}\{\text{同态}F[\alpha]\xrightarrow{\varphi}\Omega\text{满足}\varphi|_F=\varphi_0\}&\longleftrightarrow\{\varphi_0 f\in\varphi_0(F)[x]\text{在}\Omega\text{中的根}\}\\ \varphi&\longrightarrow\varphi(\alpha)\\ \big(\varphi:\alpha\mapsto x_0;\beta\mapsto\varphi_0(\beta),\beta\in F\big)&\longleftarrow x_0.\end{aligned}$$

特别，(2) 中所给出的两个集合只有有限阶，故元素个数相等.

命题 18 设 E/F 为有限扩张，则 E 是 F 的代数扩张. 反过来，若 E 由 F 及其上有限个代数元生成，则 E/F 是有限扩张.

证明思路 反证法.■

推论 19 (1) 若 E 在 F 上代数，则对任意满足 $F\subseteq R\subseteq E$ 的子环 R，R 均是域；

(2) 设有域 $F\subseteq E\subseteq L$. 若 L 在 E 上代数且 E 在 F 上代数，则 L 在 F 上代数.

证明思路 (1) 设代数元 $\alpha\in R$，由命题 16，域 $F[\alpha]=F(\alpha)\subseteq R$. 因此 $\alpha^{-1}\in R$；(2) 任意 $\alpha\in L$ 都是某个首一多项式 $x^m+a_{m-1}x^{m-1}+\cdots+a_0\in E[x]$ 的根，因此域扩张 $F[a_0,\cdots,a_{m-1},\alpha]\supseteq F[a_0,\cdots,a_{m-1}]\supseteq F[a_0,\cdots,a_{m-2}]\supseteq\cdots\supseteq F$ 有限，故是代数扩张，即 α 在 F 上代数.■

现在我们来介绍域扩张的一个简单应用：尺规作图. 当然我们得先给出尺规作图的定义：

定义 20(尺规作图) 给定一个单位长度，事先约定一些 $\mathbb{R}$ 中的点 (称它们可尺规作出). 在这个基础上，迭代地定义：一个实数称为**可尺规作出的** (即作出该长度的线段)，如果它在只有如下两种作图方式的某个组合的图像交点之处：

(1)**“尺”**：连接可尺规作出的两点得到一条直线；

(2)**“规”**：以可尺规作出的点为圆心，可尺规作出的长度为半径画圆.

设 F 是 $\mathbb{R}$ 的子域 ($F\times F\subseteq\mathbb{R}\times\mathbb{R}$ 称为 **F-平面**，其中的点称为 **F-点**)，正数 $a\in F$. 以 $\sqrt{a}$ 记 a 在 $\mathbb{R}$ 中的算术平方根. 所谓 **F-直线**就是指连接两个 F-点的 $\mathbb{R}$ 中的直线；**F-圆**就是指以 F-点为圆心，F 中的数为半径画的 $\mathbb{R}$ 中的圆.

引理 21 设 $L\neq L'$ 是 F-直线，$C\neq C'$ 是 F- 圆. 则：

(1)$L\cap L'=\varnothing$ 或 $L\cap L'$ 只有某一个 F-点；

(2)$L\cap C=\varnothing$ 或 $L\cap C$ 有 1-2 个 $F[\sqrt{a}]$-点 (即 $F[\sqrt{a}]$-平面中的点)，这里 $a\in F$ 是某个正数；

(3)$C\cap C'=\varnothing$ 或 $C\cap C'$ 有 1-2 个 $F[\sqrt{a}]$- 点，这里 $a\in F$ 是某个正数. 实际上这个情况可以归结到 (2) 中.

证明思路 解方程即可.■

注意 尺规作图可以理解为就是域扩张. 引理 21 不过是在告诉我们这个域扩张究竟会扩进去什么样的点.

现规定一个单位长度. 简单的几何作图告诉我们，或作为一个约定 (定义 20)，所有有理数 $\mathbb{Q}$ 都是可尺规作出的 (怎么作?). 因此接下来我们取 $\mathbb{Q}$-平面来讨论什么样的点可尺规作出 (相应地，取引理 21 中的 $F=\mathbb{Q}$).

定理 22 如果 x 和 y 都是可尺规作出的，那么 $-x,x+y,xy,x/y(y\neq0),\sqrt{x}(x>0)$ 均是可尺规作出的. 因此所有可尺规作出的数构成 $\mathbb{R}$ 的一个子域，且数 α 可尺规作出当且仅当 α 属于 $\mathbb{R}$ 的某个形如

$\mathbb{Q}[\sqrt{a_1},\cdots,\sqrt{a_r}], a_i \in \mathbb{Q}[\sqrt{a_1},\cdots,\sqrt{a_{i-1}}], a_i > 0$ 的子域.

推论 23 若数 α 是可尺规作出的，那么 α 在 $\mathbb{Q}$ 上代数，并且 $[\mathbb{Q}[\alpha]:\mathbb{Q}]$ 是 2 的幂.(这是必要条件，充分条件见命题 54)

证明思路 由命题 10 与定理 22，$[\mathbb{Q}[\alpha]:\mathbb{Q}]|[\mathbb{Q}[\sqrt{a_1}]\cdots[\sqrt{a_r}]:\mathbb{Q}] = [\mathbb{Q}[\sqrt{a_1},\cdots,\sqrt{a_r}]:\mathbb{Q}]$，后者是 2 的幂. 由命题 18 知 α 在 $\mathbb{Q}$ 上代数.■

至此我们已经可以给经典的三大尺规作图难题 (倍立方、三等分角、化圆为方) 下一个否定的结论：

推论 24 下述三个问题均不可尺规作出：(1)**倍立方**：找出体积为 2 个立方单位的立方体；(2)**三等分角**：将给定角三等分；(3)**化圆为方**：找出面积为 π 个平方单位的正方形.

证明思路 (1) 实数 $\sqrt[3]{2}$ 的极小多项式 x^3-2 给出 $[\mathbb{Q}[\sqrt[3]{2}]:\mathbb{Q}]=3$，因此不满足推论 23，故 $\sqrt[3]{2}$ 不可尺规作出；(2) 由三倍角公式 $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$，考虑多项式方程 $4x^3-3x-A=0$(A 为给定常数)，可以适当选取 A 使该多项式不可约，因此扩张次数仍为 3，不满足推论 23；(3)$\pi, \sqrt{\pi}$ 均是超越元，不满足推论 23.■

接下来，我们介绍代数闭域，为讨论分裂域做准备. 这部分内容和交换代数中整扩张相关的内容十分相近.

命题 + 定义 25(代数闭) 称多项式 f 在 $F[x]$ 中**分裂**，如果 f 能分解成 $F[x]$ 中一次因式的乘积. 设 Ω 是域，则下述说法等价：

(1)$\Omega[x]$ 中的任意非常数多项式在 $\Omega[x]$ 中分裂；

(2)$\Omega[x]$ 中的任意非常数多项式在 Ω 中至少有一个根；

(3)$\Omega[x]$ 中的任意 n 次多项式在 Ω 中有 n 个根；

(4)$\Omega[x]$ 中的任意非常数多项式的所有根仍都在 Ω 中；

(5)$\Omega[x]$ 中的多项式不可约当且仅当其次数为 1；

(6)Ω 上的任意有限次域扩张均为 Ω.

一个域 Ω 称为是**代数闭**的，如果它满足上述六条件之一. 域 Ω 称为是其子域 F 的**代数闭包**，如果 Ω 代数闭且 Ω 在 F 上代数 (沿用下面规定的记号则可以记 $\Omega = \bar{F}_\Omega$).

命题 26 设域 $E \supseteq F$. 则 $\{\alpha \in E | \alpha在F上代数\}$ 是一个域. 因此代数元之和、差、积、商仍是代数元.

证明思路 若 α, β 在 F 上代数，由命题 16 知 $F[\alpha,\beta] = F[\alpha][\beta]$ 是域. 由命题 18，$F[\alpha,\beta]/F$ 是有限扩张，因此是代数扩张.■

注意 有时我们需要讨论在给定扩张 E/F 中，E 在 F 上的代数元的性质. 命题 26 给我们提供了一种思路：我们称域 $\bar{F}_E = \{\alpha \in E | \alpha在F上代数\}$ 为F **在** E **中的代数闭包** (根据 E 的选取，$\bar{F}_E$ 不一定代数闭. 例如取 $F=\mathbb{Q}, E=\mathbb{R}$，则 $\bar{\mathbb{Q}}_\mathbb{R} = \mathbb{A}\cap\mathbb{R}$，这里 $\mathbb{A}$ 的定义见下例)，它是代数闭包这个概念在 Ω 非代数闭域时的推广. 由于子域的交仍是子域，因此在某个充分大的扩张下 (例如 $F \subseteq E \subseteq \Omega$，$\Omega$ 代数闭)，有 $\bar{F}_E = \bar{F}_\Omega \cap E$.

命题 27 设域 Ω 代数闭，F 是 Ω 的子域. 则 F 在 Ω 中的代数闭包 $\bar{F}_\Omega$ 就是 F 的代数闭包. 即就是说，Ω 不一定在 F 上代数，但总可以找到 Ω 的一个子域 $\bar{F}_\Omega \subseteq \Omega$ 使其在 F 上代数.

证明思路 只要证 $\bar{F}_\Omega$ 代数闭即可. 对任意 $x \in \Omega$，若 x 在 $\bar{F}_\Omega$ 上代数，由推论 19(2)，x 在 F 上代数. 因此 $x \in \bar{F}_\Omega$.■

例 $\mathbb{Q}$ 在 $\mathbb{C}$ 中的代数闭包记为 $\mathbb{A} \subsetneq \mathbb{C}(\sqrt{2} \in \mathbb{A}, \pi \notin \mathbb{A})$，其中的元素称为**代数数**.$\mathbb{A}, \mathbb{C}$ 均是代数闭域，但只有 $\mathbb{A}$ 才是 $\mathbb{Q}$(在 $\mathbb{C}$ 中) 的代数闭包. 因此代数闭包在某种意义下是“最小的”.

下面的定理保证了代数闭包的存在性：

定理 28(Artin) 承认选择公理之后，每个域都包含在某个更大的代数闭域当中，因此必有代数闭包.

证明思路 设 F 是任意一个域. 选取集合 S 满足 $F \subseteq S$，且 $|S| > \max\{|\mathbb{Z}|, |F|\}$(势). 考虑集合 $\{L | L \subseteq S, L/F是代数扩张\}$，在其上定义偏序关系 $\prec$: $E_1 \prec E_2$ 当且仅当 E_2/E_1 为代数扩张. 可以验证该集合在偏序 $\prec$ 下每个链都有上界，由 Zorn 引理必存在极大元，即 F 的一个代数闭包.■

定义 29(分裂域) 设多项式 $f \in F[x]$. 一个域 $E \supseteq F$ 称为**将** $f \in F[x]$ **分裂** (或$f \in F[x]$ **在** E **中分裂**)，如果 f 在 $E[x]$ 中可分解成一次因式的乘积 (f 在 $E[x]$ 中分裂)，即有表达式

$$f(x) = \alpha_0 \prod_{i=1}^{m} (x - \alpha_i), \alpha_i \in E.$$

上述 E 可以很大. 特别地，如果 $E=F[\alpha_1,\cdots,\alpha_m]$，那么则称 E 是 $f\in F[x]$ 的**分裂域** (或**根域**).

不难发现，$\prod f_i^{m_i}$ 和 $\prod f_i$ 具有相同的分裂域. 此外，根据域的封闭性及韦达定理，如果 f 在 E 中有 $\deg(f)-1$ 个根，那么 f 在 E 中分裂.

例 不可约多项式 $f(x)=x^3-2\in\mathbb{Q}[x]$ 在 $\mathbb{Q}[\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2]\cong\mathbb{Q}[\sqrt[3]{2},\mathrm{i}]$ 和 $\mathbb{C}$ 中均分裂，但只有 $\mathbb{Q}[\sqrt[3]{2},\mathrm{i}]$ 才是其分裂域. 直观来说，分裂域是使多项式在其上分裂的最小的比系数域大的域. 注意，f 在单扩张 $\mathbb{Q}[\alpha]/\mathbb{Q}$ 中不分裂，这里 $\alpha\in\{\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2\}$.

注意 分裂域的概念强烈依赖于多项式的系数域，因此定义 29 中应强调 f 的系数域. 比方考虑 $f=x^3-2$，当 $f\in\mathbb{Q}[x]$ 时其分裂域为 $\mathbb{Q}[\sqrt[3]{2},\mathrm{i}]$；当 $f\in\mathbb{R}[x]$ 时其分裂域为 $\mathbb{C}$. 这是因为分裂域必须包含系数域.

命题 30 任意多项式 $f\in F[x]$ 均有分裂域 E_f，且 $[E_f:F]\le(\deg f)!$.

证明思路 设 f 的根为 $\alpha_1,\cdots,\alpha_m$，则 $[F[\alpha_1]:F]\le m,[F[\alpha_1,\alpha_2]:F[\alpha_1]]\le m-1,\cdots,[F[\alpha_1,\cdots,\alpha_m]:F[\alpha_1,\cdots,\alpha_{m-1}]]\le 1$，因此 $[E_f:F]=[F[\alpha_1,\cdots,\alpha_m]:F]\le(\deg f)!$.■

命题 31 设首一多项式 $f\in F[x]$，E 是 $f\in F[x]$ 的分裂域. 又设域 Ω 将 f 分裂，则：

(1) 存在 F-同态 $\varphi:E\to\Omega$(这类同态的个数至多为 $[E:F]$ 个，当 f 在 Ω 中的根互异时取等).

(2) 若 E 和 Ω 均是 $f\in F[x]$ 的分裂域，那么任意 F-同态 $E\to\Omega$ 均是同构. 因此 $f\in F[x]$ 的分裂域在 F-同构的意义下唯一.

推论 32 设 E,L 均是 F 的域扩张，$[E:F]<\infty$，则：

(1)F-同态 $E\to L$ 的个数至多为 $[E:F]$ 个；

(2) 存在有限扩张 Ω/L 及 F-同态 $E\to\Omega$.

上述命题 31 和推论 32 的证明需要用到命题 17. 接下来我们开始讨论重根.

命题 33 设 $f,g\in F[x]$，Ω/F 是域扩张. 若 $r=(f,g)\in F[x]$，则 $r=(f,g)\in\Omega[x]$. 因此扩大系数域不改变公因式.

有了命题 33，我们就可以给出如下定义：

定义 34(重根) 设 $f\in F[x]$. 如果 f 在其分裂域 Ω(命题 33 保证了这里分裂域的合理性) 上可以分裂成 $f(x)=a\prod_{i=1}^r(x-\alpha_i)^{m_i}\in\Omega[x]\big(\sum_{i=1}^r m_i=\deg(f),m_i\ge1,\alpha_i$两两不同$\big)$，那么则称 α_i 是 f 的 m_i **重根**. 特别，当 $m_i=1$ 时称为**单根**.

命题 35 不可约多项式可以有重根.**例**：设 α 在 $\mathbb{F}_3$ 上超越. 易见 $\mathrm{Char}\big(\mathbb{F}_3(\alpha)\big)=3$，但对任意 $x\in\mathbb{F}_3(\alpha)$，$x^3\ne\alpha\Big($否则 $\alpha=\Big(\frac{\sum a_i\alpha^i}{\sum b_j\alpha^j}\Big)^3$，整理即得关于 α 的系数在 $\mathbb{F}_3$ 中的方程，与 α 超越矛盾$\Big)$. 此时 $f=x^3-\alpha$ 在 $\mathbb{F}_3(\alpha)[x]$ 中不可约. 考虑 $f\in\mathbb{F}_3(\alpha)[x]$ 的分裂域 E_f，在 E_f 上有 $f=(x-\beta)^3=x^3-\beta^3$(其中 $\beta^3=\alpha$，β 在 $\mathbb{F}_3(\alpha)$ 上代数). 故此不可约多项式有 3 重根 β.

我们希望确定一个多项式何时才会有重根. 不难发现这个问题只需要处理完不可约多项式的情况即可.

定义 36(微商) 设 F 是域，则 $f=\sum_{i=0}^n a_ix^i\in F[x]$ 的**微商** (或**导数**) 定义为 $f'=\sum_{i=1}^n ia_ix^{i-1}$. 特别，当 $\mathrm{Char}(F)=p(p$ 是素数) 时，$(x^p)'=0$.

下面利用微商给出不可约多项式是否有重根的判定准则：

命题 37 设非常数不可约多项式 $f\in F[x]$，则下述说法等价：

(1)f 有重根；(2)$(f,f')\ne1$；(3)F 有非零特征 p 且 f 可写成 $g(x^p)$；(4)f 的所有根都是重根.

证明思路 (1) $\Rightarrow$ (2)$f=(x-a)^mg,m>1$；(2) $\Rightarrow$ (3) 由于 f 不可约，$\deg(f')<\deg(f)$ 和 $(f,f')\ne1$ 导致 $f'|f$，并且 f' 只能是常数，进一步只能为 0(否则和 $(f,f')=1$ 矛盾). 易见这种情况只能在 F 的特征 p 非零时出现. 此时 f 可写成 x^p 的多项式；(3) $\Rightarrow$ (4) 由 $f(x)=g(x^p)$ 知 f 的根一定是 p 重根；(4) $\Rightarrow$ (1) 显然.■

推论 38 设非常数多项式 $f\in F[x]$，则 $(f,f')=1$ 当且仅当 f 只有单根.

定义 39(可分多项式) 一个多项式称为**可分**的，如果它 (在其分裂域上) 只有单根. 显然，特征为 0 域上的不可约多项式一定可分，故此定义一般用于特征非零的情况. 一个域 F 称为是**完美** (Perfect) 的，如果 $F[x]$ 中的所有不可约多项式都可分.

命题 40 域 F 完美当且仅当 $\mathrm{Char}(F)=0$，或 $\mathrm{Char}(F)=p(p$ 是素数) 且任意 F 中的元素均是 F 中某个元素的 p 次幂. 特别地，注意到有限域有 Frobenius 自同构，因此有限域都是完美的；注意到代数闭域上的多项式均在其中分裂，因此代数闭域都是完美的.

2、Galois 基本定理

定义 41 考虑域扩张 E/F，则 E 上的所有 F-自同构 $E \xrightarrow{\sim} E$ 作成一个群，记为 $\mathrm{Aut}(E/F)$.

命题 42 设 E 是可分多项式 $f \in F[x]$ 的分裂域，则 $|\mathrm{Aut}(E/F)| = [E:F]$.

证明思路 对 F-同态 $E \to E$ 用命题 31(2)，再由命题 31(1) 知结论成立.■

注意 命题 42 中，“E 是可分多项式的分裂域”这个条件不可减弱. 例如考虑单扩张 $E = F[\alpha]$，若 α 是某个多项式 $f \in F[x]$ 在 E 中唯一的根，由命题 17(2)，$|\mathrm{Aut}(E/F)| = 1$. 比方说，$\mathbb{Q}[\sqrt[3]{2}]$ 不是 $x^3 - 2 \in \mathbb{Q}[x]$ 的分裂域，$|\mathrm{Aut}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q})| = 1$.

定义 43(不动域) 设 G 是域 E 的若干自同构作成的群，称 $E^G = \mathrm{Inv}(G) = \{\alpha \in E | \forall \sigma \in G, \sigma\alpha = \alpha\}$ 为 E 在 G 下的**不动域** (容易验证 E^G 确实是 E 的子域).

定理 44(Artin) 设 G 是域 E 的有限个自同构作成的群，则 $[E:E^G] \le |G|$.

证明思路 设 $G = \{\sigma_1 = \mathrm{id}, \sigma_2, \cdots, \sigma_n\}$，$u_1, \cdots, u_{n+1}$ 为 E 中全不为零的 $n+1$ 个元素. 用 σ_i 作用 u_j 得 $n \times (n+1)$ 级矩阵

$$\Gamma = \begin{pmatrix} \sigma_1(u_1) & \sigma_1(u_2) & \cdots & \sigma_1(u_{n+1}) \\ \sigma_2(u_1) & \sigma_2(u_2) & \cdots & \sigma_2(u_{n+1}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(u_1) & \sigma_n(u_2) & \cdots & \sigma_n(u_{n+1}) \end{pmatrix},$$

其列向量 $\alpha_1, \cdots, \alpha_{n+1}$ 在 E 上线性相关 ($\Gamma X = O$ 有非零解)，于是存在极大无关组 $\alpha_1, \cdots, \alpha_r$，故 $\alpha_{r+1} = k_1\alpha_1 + \cdots + k_r\alpha_r$ 且表法唯一，即 $\sigma_i(u_{r+1}) = k_1\sigma_i(u_1) + \cdots + k_r\sigma_i(u_r), i = 1, \cdots, n$. 用 $\tau \in G$ 作用上式得 $\tau\sigma_i(u_{r+1}) = \tau(k_1)\tau\sigma_i(u_1) + \cdots + \tau(k_r)\tau\sigma_i(u_r), i = 1, \cdots, n$. 注意到 G 是有限群，$\{\tau\sigma_1, \cdots, \tau\sigma_n\}$ 是 G 中元素的某个排列，将上式调换顺序并写成向量形式得 $\alpha_{r+1} = \tau(k_1)\alpha_1 + \cdots + \tau(k_r)\alpha_r, \forall \tau \in G$. 因此 $\tau(k_j) = k_j$，即 $k_j \in E^G$. 由 $u_{r+1} = k_1u_1 + \cdots + k_ru_r$ 知 $u_1, \cdots, u_{r+1}$ 在 E^G 上线性相关，故 $u_1, \cdots, u_{n+1}$ 也在 E^G 上线性相关，因此 $\dim_{E^G}(E) \le n$.■

推论 45 设 G 是域 E 的有限个自同构作成的群，则 $G = \mathrm{Aut}(E/E^G)$.

证明思路 显然 $G \subseteq \mathrm{Aut}(E/E^G)$. 由定理 44 和推论 32(1)，$[E:E^G] \le |G| \le |\mathrm{Aut}(E/E^G)| \le [E:E^G]$.■

定义 46(可分正规) 一个代数扩张 E/F 称为**可分扩张**，如果 E 中任意元素 e 的极小多项式 $f_e \in F[x]$ 可分. 一个代数扩张 E/F 称为**正规扩张**，如果 E 中任意元素 e 的极小多项式 $f_e \in F[x]$ 在 E 中分裂.

例 $\mathbb{F}_p(\alpha)/\mathbb{F}_p(\alpha^p)$ 不是可分扩张，因为 α 的极小多项式 $x^p - \alpha^p \in \mathbb{F}_p(\alpha^p)[x]$ 的根为 p 重根；$\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ 不是正规扩张，因为 $\sqrt[3]{2}$ 的极小多项式 $x^3 - 2 \in \mathbb{Q}[x]$ 在 $\mathbb{Q}[\sqrt[3]{2}]$ 中不分裂.

命题 47 (1) 若任意在 E 中有根的不可约多项式 $f \in F[x]$ 可分，则 E/F 是可分扩张.

(2) 代数扩张 E/F 正规当且仅当任意不可约多项式 $f \in F[x]$，只要 f 在 E 中有一根，那么 f 的全部根均在 E 中 (即 f 在 $E[x]$ 中分裂).

注意 设 $f \in F[x]$ 是 m 次不可约多项式，E/F 是代数扩张，若 f 在 E 中有根，则：

$$\left.\begin{array}{r} E/F\text{可分} \Rightarrow f\text{无重根} \\ E/F\text{正规} \Rightarrow f\text{在}E\text{中分裂} \end{array}\right\} \Rightarrow f\text{在}E\text{中有}m\text{个不同根},$$

因此代数扩张 E/F 可分正规 $\Leftrightarrow$ E 中任意元素 e 的极小多项式 $f_e \in F[x]$ 在 E 中有 $[F[e]:F]$ 个不同根.

命题 + 定义 48(Galois 扩张) 域扩张 E/F 称为 **Galois 扩张**，如果它满足下述等价的四个条件之一：

(1)$[E:F] < \infty$ 且 $E^{\mathrm{Aut}(E/F)} = F$.

(2)E 是某个可分多项式 $f \in F[x]$ 的分裂域.

(3) 存在 E 的有限阶自同构群 G，使 $F = E^G$.

(4)$[E:F] < \infty$ 且 E/F 可分正规.

当 E/F 是 Galois 扩张时，有限群 $\mathrm{Aut}(E/F)$ 称为 E 在 F 上的 **Galois 群**，记为 $\mathrm{Gal}(E/F)$. 特别地，若 $\mathrm{Gal}(E/F)$ 是 Abel 群或循环群，则称 E/F 为 **Abel 扩张**或**循环扩张**.

推论 49 任意有限的可分扩张 E/F 均包含在 F 的某个 Galois 扩张当中.

证明思路 设 $E=F[\alpha_1,\cdots,\alpha_m], f_i\in F[x]$ 是 α_i 的极小多项式. 根据命题 48(2)，此时可分多项式 $\prod_{f_i\neq f_j} f_i\in F[x]$ 的分裂域就是 F 的一个 Galois 扩张，它包含 E.■

推论 50 设域 $F\subseteq E\subseteq K$，若 K/F 是 Galois 扩张，则 K/E 也是 Galois 扩张 (E/F 不一定是).

证明思路 K 是某个可分多项式 $f\in F[x]$ 的分裂域，注意到 $K=F[\alpha_1,\cdots,\alpha_m]=E[\alpha_1,\cdots,\alpha_m]$，因此它是 $f\in E[x]$ 的分裂域.■

定理 51(Galois 基本定理) 设 E/F 是 Galois 扩张，则存在一一对应：

$$\begin{aligned}\{\mathrm{Gal}(E/F)\text{的子群}\}&\longleftrightarrow\{E/F\text{的中间域}\}\\ H\ ;\ \sigma H\sigma^{-1}&\longrightarrow E^H\ ;\ \sigma(E^H)\\ \mathrm{Gal}(E/L)\ ;\ \sigma\,\mathrm{Gal}(E/L)\sigma^{-1}&\longleftarrow L\ ;\ \sigma(L).\end{aligned}$$

其中 $\sigma\in\mathrm{Gal}(E/F)$. 此外，还有：

(1) 上述对应满足 $H_1\supseteq H_2\Leftrightarrow E^{H_1}\subseteq E^{H_2}$(反变)，且 $(H_1:H_2)=[E^{H_2}:E^{H_1}]$.

(2) 对任意 $\sigma\in\mathrm{Gal}(E/F)$，$E^{\sigma H\sigma^{-1}}=\sigma(E^H),\mathrm{Gal}(E/\sigma L)=\sigma\,\mathrm{Gal}(E/L)\sigma^{-1}$.

(3)H 是 $\mathrm{Gal}(E/F)$ 的正规子群 $\Leftrightarrow E^H/F$ 是正规 (Galois) 扩张. 此时商群 $\mathrm{Gal}(E/F)\big/H\cong\mathrm{Gal}(E^H/F)$.

证明思路 由定义 48 和推论 45 有 $E^{\mathrm{Gal}(E/L)}=L$ 和 $\mathrm{Gal}(E/E^H)=H$(推论 50 保证 E/L 和 E/E^H 是 Galois 的). 通过这两个等式不难发现上述对应确实是可逆的.(1) 前半部分可直接验证，后半部分由于有域扩张 $E^{H_1}\subseteq E^{H_2}\subseteq E$ 且 E/F 是正规扩张，根据命题 42 有

$$[E^{H_2}:E^{H_1}]=\frac{[E:E^{H_1}]}{[E:E^{H_2}]}=\frac{|\,\mathrm{Gal}(E/E^{H_1})|}{|\,\mathrm{Gal}(E/E^{H_2})|}=\frac{|H_1|}{|H_2|}=(H_1:H_2),$$

故 (1) 成立；(2) 由 (1) 可得；由 (2)，对任意 $\sigma\in\mathrm{Gal}(E/F)$，$\sigma(E^H)=E^H$，因此有群同态 $\varphi:\mathrm{Gal}(E/F)\to\mathrm{Aut}(E^H/F),\sigma\mapsto\sigma|_{E^H}$. 根据不动域的定义 43，有 $\ker\varphi=H$. 此时 $F=(E^H)^{\mathrm{Gal}(E/F)\big/H}=(E^H)^{\mathrm{Aut}(E^H/F)}$，由命题 48(3)，$E^H/F$ 是正规 (Galois) 扩张.■

技术性来说，命题 42、推论 45、命题 48、推论 50、定理 51 在涉及 Galois 扩张的时候经常会用到，应特别留意.

注意 设 $L_1,\cdots,L_r$ 是 Galois 扩张 E/F 的中间域，记 $H_i=\mathrm{Gal}(E/L_i)$. 根据定义 14，$L_1\cdots L_r$ 是包含了 $L_1,\cdots,L_r$ 的最小的域，因此 $\mathrm{Gal}(E/L_1\cdots L_r)$ 应该为包含在 $H_1,\cdots,H_r$ 中最大的子群：$\bigcap H_i$.

设 H 是 $G=\mathrm{Gal}(E/F)$ 的子群，易证包含在 H 中的最大的正规子群应为 $N=\bigcap_{\sigma\in G}\sigma H\sigma^{-1}$. 此时 E^N/F 是最小的包含 E^H 的正规 (Galois) 扩张. 注意到 $N=\bigcap_{\sigma\in G}\sigma H\sigma^{-1}=\mathrm{Gal}\big(E/\bullet_{\sigma\in G}\sigma(E^H)\big)$，其中 $\bullet$ 代表复合域，因此有 $E^N=\bullet_{\sigma\in G}\sigma(E^H)$. 这里 E^N 称为**E^H 在 E 中的正规 (Galois) 闭包**.

以下两个命题中出现的域必须是某个很大的域的子域，这样可以保证子域的交仍是子域.

命题 52 设 E/F 是 Galois 扩张，L/F 是域扩张，则 $E\cdot L/L$，$E/E\cap L$ 均是 Galois 扩张，且有同构 $\varphi:\mathrm{Gal}(E\cdot L/L)\xrightarrow{\sim}\mathrm{Gal}(E/E\cap L),\sigma\mapsto\sigma|_E$. 此外，若 $[L:F]<\infty$，则 $[E\cdot L:F]=\frac{[E:F][L:F]}{[E\cap L:F]}$.

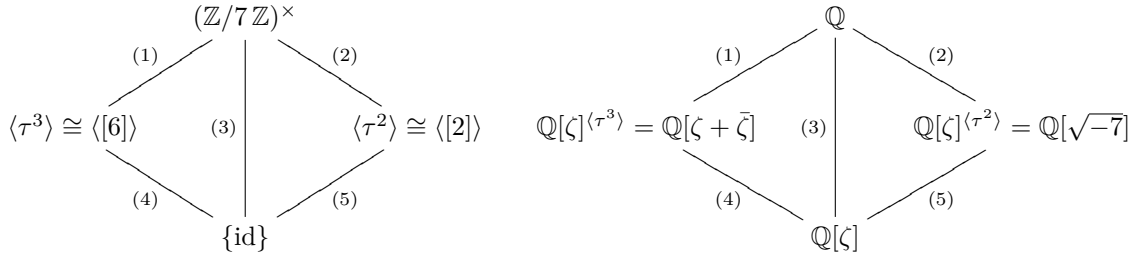
证明思路 根据定义 48(2)，注意到分裂域为 E 的可分多项式 $f\in F[x]$ 看成 $f\in L[x]$ 的分裂域为 $E\cdot L$(包含 E,L 最小的域). 因此 $E\cdot L/L$ 是 Galois 扩张，$E/E\cap L$ 同理. 易证 $\sigma(E)=E$，故 σ 可限制在 E 上 (良好定义). 又注意到 $E\cap L=E^{\mathrm{Gal}(E\cdot L/L)}$，由推论 45，有 $\mathrm{Gal}(E\cdot L/L)\cong\mathrm{Gal}(E/E^{\mathrm{Gal}(E\cdot L/L)})\cong\mathrm{Gal}(E/E\cap L)$. 由 $|\,\mathrm{Gal}(E\cdot L/L)|=|\,\mathrm{Gal}(E/E\cap L)|$ 及定理 51(1) 即得后面的等式.■

命题 53 设 E_1/F，E_2/F 均是 Galois 扩张，则 $E_1\cdot E_2/F$，$E_1\cap E_2/F$ 也都是 Galois 扩张，且有群同构 $\varphi:\mathrm{Gal}(E_1\cdot E_2/F)\xrightarrow{\sim}\big\{(\sigma_1,\sigma_2)\big|\sigma_1|_{E_1\cap E_2}=\sigma_2|_{E_1\cap E_2}\big\}\subseteq\mathrm{Gal}(E_1/F)\times\mathrm{Gal}(E_2/F),\sigma\mapsto(\sigma|_{E_1},\sigma|_{E_2})$.

例 本例来源于 [1] 例 3.21，置于此处只是为了理解定理 51. 考虑域扩张 $\mathbb{Q}[\zeta]/\mathbb{Q}$，其中 $\zeta=e^{2\pi\,\mathrm{i}/7}$.$\zeta$ 的极小多项式为 $f=x^6+x^5+x^4+x^3+x^2+x+1\in\mathbb{Q}[x]$，它可分 (定义 39)，且分裂域就是 $\mathbb{Q}[\zeta]$，因此 $\mathbb{Q}[\zeta]/\mathbb{Q}$ 是 Galois 扩张 (定义 48.2). 显然 $[\mathbb{Q}[\zeta]:\mathbb{Q}]=6$. 可以验证 $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})\xrightarrow{\sim}(\mathbb{Z}/7\,\mathbb{Z})^\times,\sigma\mapsto[n](\sigma:\zeta\mapsto\zeta^n,n=1,\cdots,6)$ 是一个群同构. 注意到 $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ 或 $(\mathbb{Z}/7\,\mathbb{Z})^\times$ 都是循环群，对应生成元是 $\tau:\zeta\mapsto\zeta^3$ 或 $[3]$. 考虑

$\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ 中的子群 $\langle\tau^3\rangle$ 和 $\langle\tau^2\rangle$，亦即考虑 $(\mathbb{Z}/7\mathbb{Z})^\times$ 中的子群 $\langle[6]\rangle=\{[1],[6]\}$ 和 $\langle[2]\rangle=\{[1],[2],[4]\}$. 有了这些子群，我们可以得到：下图中，(1) 和 (5) 的次数是 3，(2) 和 (4) 的次数是 2，(3) 的次数是 6. 由推论 50，(3)、(4) 和 (5) 均是 Galois 扩张 (实际上显然 $\{\mathrm{id}\}$ 是任意群的正规子群，利用定理 51(3) 也可以得到这个结论). 此外，(1) 和 (2) 也是 Galois 扩张：注意到 $\langle\tau^3\rangle=\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}[\zeta]^{\langle\tau^3\rangle})$ 是 $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ 的正规子群 (由于 $\tau^3\zeta=\zeta^6=\bar{\zeta}$，故 $\mathbb{Q}[\zeta]^{\langle\tau^3\rangle}\supseteq\mathbb{Q}[\zeta+\bar{\zeta}]$，观察次数可得 $\mathbb{Q}[\zeta]^{\langle\tau^3\rangle}=\mathbb{Q}[\zeta+\bar{\zeta}]$)，由定理 51(3)，$\mathrm{Gal}(\mathbb{Q}[\zeta+\bar{\zeta}]/\mathbb{Q})=\frac{\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})}{\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}[\zeta+\bar{\zeta}])}=(\mathbb{Z}/7\mathbb{Z})^\times/\langle[6]\rangle$.

可以利用韦达定理求出：(1) 对应的极小多项式是 x^3+x^2-2x-1，(2) 对应的极小多项式是 x^2+7.



之前我们已经讨论过尺规作图并且给出了某个实数可尺规作出的必要条件 (推论 23). 现在我们亦可给出一个充分条件 (命题 54)，它在理论上可以解答 Gauss 为何可以作出正 17 边形 (推论 55).

命题 54 若 α 包含在 $\mathbb{R}$ 的一个子域 E 中，且 $E/\mathbb{Q}$ 是次数为 2^r 的 Galois 扩张，则 α 可尺规作出.

证明思路 $|\mathrm{Gal}(E/\mathbb{Q})|=2^r$. 由于有限 p-群可解，因此存在正规子群链 $\{\mathrm{id}\}=G_0\subseteq G_1\subseteq\cdots\subseteq G_r=\mathrm{Gal}(E/\mathbb{Q})$ 满足 $G_i/G_{i-1}=2$. 此时有对应的域塔 $E=E_0\supseteq E_1\supseteq\cdots\supseteq E_r=\mathbb{Q}$，$[E_i:E_{i+1}]=2$. 易证二次扩张 ($\mathrm{Char}\neq2$)$E/F$ 必可找到 $a\in F$ 使得 $E=F[\sqrt{a}]$(求二次极小多项式的根即可)，因此 $\alpha\in E$ 可通过不断二次域扩张作出.■

推论 55 若 p 是 2^k+1 型素数，则 $\cos\frac{2\pi}{p}$ 可尺规作出. 因此正 $p=2^k+1$ 边形可尺规作出.

证明思路 注意到 $\mathbb{Q}[e^{2\pi\,\mathrm{i}/p}]/\mathbb{Q}$ 是 Galois 扩张且 $\mathrm{Gal}(\mathbb{Q}[e^{2\pi\,\mathrm{i}/p}]/\mathbb{Q})\cong(\mathbb{Z}/p\mathbb{Z})^\times$(例如见上例)，$[\mathbb{Q}[e^{2\pi\,\mathrm{i}/p}]:\mathbb{Q}]=|(\mathbb{Z}/p\mathbb{Z})^\times|=2^k$. 由于 $\mathbb{Q}[\cos\frac{2\pi}{p}]\subseteq\mathbb{Q}[e^{2\pi\,\mathrm{i}/p}]$，根据命题 10 及命题 52，$\mathbb{Q}[\cos\frac{2\pi}{p}]/\mathbb{Q}$ 是次数整除 2^k 的 Galois 扩张. 再应用命题 54 即可.■

定义 56(Galois 群) 记可分多项式 $f\in F[x]$ 的分裂域为 F_f，则 F_f/F 是 Galois 扩张. 此时称 $\mathrm{Gal}(F_f/F)$ 为 $f\in F[x]$ 的 **Galois 群**，记为 G_f. 设 f 在 F_f 中的根为 $S=\{\alpha_1,\cdots,\alpha_n\}$，则对任意 $\sigma\in G_f$，$\sigma S=S$ 是一个置换. 因此 G_f 是 S_n 的一个子群. 特别地，有：

命题 57 $G_f=\{\sigma\in S_n|$ 对任意满足 $p(\alpha_1,\cdots,\alpha_n)=0$ 的 $p\in F[x_1,\cdots,x_n]$，均有 $p(\sigma\alpha_1,\cdots,\sigma\alpha_n)=0\}$.

证明思路 设 σ 满足等号右边. 对任意 $\alpha\in F_f$，α 可表成 $\alpha=f(\alpha_1,\cdots,\alpha_n)$，这里 $f\in F[x_1,\cdots,x_n]$. 定义 $\sigma':F_f\to F_f,\alpha\mapsto f(\sigma\alpha_1,\cdots,\sigma\alpha_n)$. 易证这里 σ' 是良好定义的 (与 α 表法无关) 且由 α 唯一确定. 此时可以验证 σ' 是 F-同构 (保持运算显然，满射是因为 $F_f=F[S]=F[\sigma S]$，单射显然). ■

上述命题就是说，确定了根的置换关系之后可以把这个关系提升为分裂域之间的 F-同态，而这里所谓的“置换关系”就是命题 57 中描述的.

Galois 理论的重要影响之一就是回答了“高次方程是否可根式解”这个问题. 我们首先搞明白什么是“可根式解”，然后再给出主要定理.

定义 58 设多项式 $f\in F[x]$. 称方程 $f(x)=0$ **可根式解**，如果存在域塔 (称为**根式扩张**)$F=F_0\subseteq F_1\subseteq\cdots\subseteq F_m$，满足：$F_i=F_{i-1}[\alpha_i]$(其中 $\alpha_i^{m_i}\in F_{i-1}$，这称为**单根式扩张**) 且 f 的分裂域 $F_f\subseteq F_m$.

定理 59(Galois) 设 F 是特征为 0 的域，$f\in F[x]$，则方程 $f(x)=0$ 可根式解当且仅当群 G_f 可解.

命题 60(可解群的性质) 至此我们有必要给出一些关于可解群的命题：

(1) 群 G 是可解的当且仅当存在递降的子群列 $G=G_0\rhd G_1\rhd\cdots\rhd G_s=\{\mathrm{id}\}$，其中 G_{i-1}/G_i 交换.

(2) 有限群 G 可解当且仅当存在递降的子群列 $G=G_0\rhd G_1\rhd\cdots\rhd G_s=\{\mathrm{id}\}$，其中 G_{i-1}/G_i 都是素数阶的循环群.

(3) 当 $n>4$ 时，S_n 不可解 (因为此时 A_n 是单群)；当 $n\leq4$ 时，S_n 可解.

(4)Abel 群一定可解；可解群的子群、同态像、直积仍可解；若有群正合列 $1\to H\to G\to M\to1$ 且

H, M 可解，则 G 可解.

引理 61 设 p 是素数，若域 F 包含 p 个不同的 p 次单位根，则 F 上任意一个 p 次循环扩张 E/F 是根式扩张 (证明要用到 **Lagrange 预解式**).

注意 以 3 次扩张 E/F 为例，我们来看看定理 59 在此特殊情形下的阐释.(情况一) 若三次单位根 $\zeta \in F$，由引理 61 知 E/F 是 3 次根式扩张，故 $f(x)=0$ 可根式解；(情况二) 若三次单位根 $\zeta \notin F$，首先作域扩张 $F \subseteq F[\zeta]$，这是一个 2 次扩张 (极小多项式 $x^2+x+1=0$) 且是单根式扩张 ($\zeta^3=1$)，再作域扩张 $F[\zeta] \subseteq E[\zeta]$，根据引理 61 这也是 3 次根式扩张，因此对根式扩张 $F \subseteq F[\zeta] \subseteq E[\zeta]$ 而言有 $E \subseteq E[\zeta]$，故根据定义 58，$f(x)=0$ 可根式解. 仿此利用数学归纳法，稍加启发便得到定理 59 充分性的证明：

定理 59 充分性的证明思路 设 $f \in F[x]$ 的分裂域为 F_f. 对 $[F_f : F]$ 做归纳法，假设 $[F_f : F] < n$ 时命题成立. 当 $[F_f : F] = n$ 时，设 n 的素因子为 $p_1, \cdots, p_t$，ζ 是一个 $l = p_1 \cdots p_t$ 次单位根，则 $\mathrm{Gal}(F[\zeta]/F)$ 是 Abel 群，故可解. 由于 $[F[\zeta] : F] \leq \varphi(l) < n$(这里 φ 是 Euler 函数，$\varphi(p_i) = p_i - 1$ 且 $\varphi(p_1 \cdots p_t) = \varphi(p_1) \cdots \varphi(p_t)$)，根据归纳假设，存在根式扩张 $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m$，$F[\zeta] \subseteq F_m$. 由命题 52，此时 $H = \mathrm{Gal}(F_f \cdot F_m/F_m) = \mathrm{Gal}(F_f/F_f \cap F_m)$ 是 $G_f = \mathrm{Gal}(F_f/F)$ 的一个子群 (考虑复合域 $F_f \cdot F_m$ 是为了在 F_m 上建立起 f 的分裂域)，根据命题 60 它可解. 于是 H 有合成群列 $H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_r$，$H_{i-1}/H_i$ 是素数阶循环群. 由定理 51，存在一一对应 $\{F_f \cdot F_m/F_m \text{ 的中间域 }\} \longleftrightarrow \{H \text{ 的子群}\}$，得到 $F_f \cdot F_m$ 的子域链 $F_m \subseteq F_m^1 \subseteq \cdots \subseteq F_f \cdot F_m$，使得 F_m^i/F_m^{i-1} 是 Galois 扩张且 $\mathrm{Gal}(F_m^i/F_m^{i-1}) = H_{i-1}/H_i$. 因为 $|H_{i-1}/H_i||H_{i-1}||H||G_f| = n$，所以 H_{i-1}/H_i 的阶在 $\{p_1, \cdots, p_t\}$ 中取得 (对应 F_m^i/F_m^{i-1} 就是 p_k 次循环扩张)，又因为 $F_m \supseteq F[\zeta] \supseteq F[\zeta_{p_k}]$，根据引理 61，上面的子域链 $F_m \subseteq F_m^1 \subseteq \cdots \subseteq F_f \cdot F_m$ 是根式扩张 (直观上可以理解为可解群拉出的合成群列给出根式扩张). 将已有的两条子域链接起来得 $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m \subseteq F_m^1 \subseteq \cdots \subseteq F_f \cdot F_m$，这就是我们要的根式扩张，并且有 $F_f \subseteq F_f \cdot F_m$.■

例 (1) 考虑 $f(x) = x^4 - x^2 - 2 \in \mathbb{Q}[x]$(它的根为 $\pm\sqrt{2}, \pm \mathrm{i}$). 由定理 63 知 $G_f = \langle (13), (1234) \rangle$，它是可解群. 由定义 58，$f(x)=0$ 可根式解.

(2) 考虑 $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$，可以计算 $G_f = S_5$ 不可解，故 $f(x)=0$ 不可根式解.

3、计算及应用

► 问题 I：四次方程 Galois 群的刻画

定义 + 定理 62(预解) 设多项式 f 在其分裂域上有根 $\{\alpha_1, \cdots, \alpha_n\}$，称表达式 $D(f) = \prod\limits_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$ 为 f 的**判别式**(需验证良好定义，即对根的任意编号不影响 $D(f)$ 的值). 对四次多项式 $f = x^4 + ax^3 + bx^2 + cx + d$ 而言，称多项式 $g = x^3 - bx^2 + (ac - 4d)x + 4bd - a^2d - c^2$ 为它的**预解式**. 可以证明 $D(f) = D(g)$.

定理 63 设域 F 的特征不为 2，又设 $f \in F[x]$ 为一个 4 次不可约多项式，g 为它的 3 次预解式，E 为 $g \in F[x]$ 的分裂域. 则：

(1) 若 g 不可约且 $\sqrt{D(g)} \notin F$，则 $G_f \cong S_4$，$[E : F] = 6$；

(2) 若 g 不可约且 $\sqrt{D(g)} \in F$，则 $G_f \cong A_4$，$[E : F] = 3$；

(3) 若 g 有一个 2 次不可约因式且 f 在 E 上不可约，则

$$G_f \cong \langle (13), (1234) \rangle = \{\mathrm{id}, (13), (1234), (13)(24), (1432), (12)(34), (24), (14)(23)\}, [E : F] = 2;$$

(4) 若 g 有一个 2 次不可约因式且 f 在 E 上可约，则 $G_f \cong \langle (1234) \rangle \cong \mathbb{Z}/4\,\mathbb{Z}$，$[E : F] = 2$；

(5) 若 g 完全可分解成一次因式之积，则

$$G_f \cong \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}, [E : F] = 1.$$

► 问题 II：有限域

命题 64 有限域上的任意有限扩张都是单扩张.

证明思路 注意到有限域的有限扩张仍为有限域，且有限域的乘法子群是循环群即可 (这是初等数论中的一个简单命题).■

设 E 是特征为 p 的有限域，$[E:\mathbb{F}_p]=n$. 显然 $|E|=p^n, |E^\times|=p^n-1$. 根据 Lagrange 定理，$E^\times$ 中的元素全部都是 $x^{p^n-1}-1$ 的根，亦即 E 中的元素全部都是 $x^{p^n}-x$ 的根，故 E 是 $x^{p^n}-x\in\mathbb{F}_p[x]$ 的分裂域. 根据命题 31(2)，含有同样多元素的有限域在同构的意义下唯一 (不一定是典范同构). 另一方面，由于 $(x^{p^n}-x)'=-1$，根据命题 37，它 (在其分裂域上) 无重根. 故 E 实际上就是 $x^{p^n}-x\in\mathbb{F}_p[x]$ 所有根作成的域. 综上我们得到如下定理：

定理 65 对任意正整数 n，总存在含有 p^n 个元素的域 (记为 $\mathbb{F}_{p^n}$). 实际上 (在同构意义下) 它就是 $x^{p^n}-x\in\mathbb{F}_p[x]$ 的分裂域. 此外，$\mathbb{F}_{p^n}/\mathbb{F}_p$ 是循环 Galois 扩张，且 $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ 由 Frobenius 自同构 $\sigma:a\mapsto a^p$ 生成.

证明思路 之前已经阐明 $\mathbb{F}_{p^n}$ 是可分多项式 $x^{p^n}-x\in\mathbb{F}_p[x]$ 的分裂域，因此 $\mathbb{F}_{p^n}/\mathbb{F}_p$ 是 Galois 扩张. 由命题 42，$|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)|=[\mathbb{F}_{p^n}:\mathbb{F}_p]=n$. 而 Frobenius 自同构 $\sigma:\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}, a\mapsto a^p$ 是 $\mathbb{F}_p$- 自同构 (Femart 小定理)，且它恰好可以生成一个 n 阶群 ($\sigma^n=\mathrm{id}$).■

推论 66 设 E 是含有 p^n 个元素的域，则对 n 的任意因子 m，E 包含且只包含了一个含有 p^m 个元素的域.

证明思路 考虑 n 阶循环群 $\mathrm{Gal}(E/\mathbb{F}_p)=\langle\sigma:a\mapsto a^p\rangle$. 设 $m|n$，则 $\mathrm{Gal}(E/\mathbb{F}_p)$ 有唯一 (因为循环)$\frac{n}{m}$ 阶正规子群 $\langle\sigma^m\rangle$. 根据 Galois 基本定理 (定理 51)，$E/E^{\langle\sigma^m\rangle}$ 就是一个 $[E:E^{\langle\sigma^m\rangle}]=|\mathrm{Gal}(E/E^{\langle\sigma^m\rangle})|=|\langle\sigma^m\rangle|=\frac{n}{m}$ 次域扩张，因此 $E^{\langle\sigma^m\rangle}/\mathbb{F}_p$ 是一个 $[E^{\langle\sigma^m\rangle}:\mathbb{F}_p]=\frac{[E:\mathbb{F}_p]}{[E:E^{\langle\sigma^m\rangle}]}=\frac{n}{n/m}=m$ 次域扩张，即 $|E^{\langle\sigma^m\rangle}|=p^m$.■

注意到代数闭域一定含有无穷多个元素 (为什么?)，实际上我们已经证明了如下定理：

定理 67 设 $\bar{\mathbb{F}}_p$ 是 $\mathbb{F}_p$ 的代数闭包，则 $\bar{\mathbb{F}}_p$ 包含且只包含了一个含有 p^n 个元素的域 (这里任给 $n\geq 1$)，即 $x^{p^n}-x\in\mathbb{F}_p[x]$ 的分裂域. 此外，$\mathbb{F}_{p^m}\subseteq\mathbb{F}_{p^n}$ 当且仅当 $m|n$.

► **问题 III：迹与范数** (主要参考文献 [1]Chapter5.12 和 [10]Chapter1.2)

线性代数里面迹与范数的概念可以在域扩张的理论框架下推广，这是因为域总是其子域上的线性空间. 设 E/F 是次数为 n 的域扩张，任意 $\alpha\in E$ 总诱导一个 F- 线性空间 E 上的线性变换 $\alpha_L:E\to E, x\mapsto\alpha x$.

定义 68(迹与范数) 对于任给 $\alpha\in E$，定义如下 3 个相似不变量：

(1) 定义 α 的**迹**$\mathrm{Trace}_{E/F}(\alpha)=\mathrm{Trace}(\alpha_L)$，即线性变换 α_L(在某一组基下的矩阵) 的迹；

(2) 定义 α 的**范数**$\mathrm{Norm}_{E/F}(\alpha)=\det(\alpha_L)$，即线性变换 α_L(在某一组基下的矩阵) 的行列式；

(3) 定义 α 的**特征多项式**$\lambda_{E/F}(\alpha,x)$ 为线性变换 α_L(在某一组基下的矩阵) 的特征多项式.

可以验证，$\mathrm{Trace}_{E/F}(\cdot):(E,+)\to(F,+)$、$\mathrm{Norm}_{E/F}(\cdot)|_{E^\times}:(E^\times,\cdot)\to(F^\times,\cdot)$ 均是群同态.

例 对域扩张 E/F 而言，若 $\alpha\in F$，此时 $\mathrm{Trace}_{E/F}(\alpha)=n\alpha$，$\mathrm{Norm}_{E/F}(\alpha)=\alpha^n$，$\lambda_{E/F}(\alpha,x)=(x-\alpha)^n$，其中 $n=[E:F]$.

命题 69 设 E/F 是有限扩张，f 是 $\alpha\in E$ 在 F 上的极小多项式，则 $\lambda_{E/F}(\alpha,x)=f^{[E:F[\alpha]]}$.

证明思路 首先考虑 $E=F[\alpha]$ 的情况. 由 Hamilton-Caylay 定理知 $\lambda_{E/F}(\alpha,\alpha)=0$，因此 $f(x)|\lambda_{E/F}(\alpha,x)$. 而它们都是次数为 $[E:F]$ 的首一多项式，故 $\lambda_{E/F}(\alpha,x)=f(x)$. 一般地，对 $F\subseteq F[\alpha]\subseteq E$ 而言，设 F-线性空间 $F[\alpha]$ 的基为 $\beta_1,\cdots,\beta_n$，$F[\alpha]$-线性空间 E 的基为 $\gamma_1,\cdots,\gamma_m$. 设 F-线性变换 $\alpha_L:E\to E, x\mapsto ax$ 的限制映射 $\alpha_L|_{F[\alpha]}$ 在基 $\{\beta_i|1\leq i\leq n\}$ 下的矩阵为 $B=(b_{ij})$，前面已经证明了 B 的特征多项式为 f. 注意到 F-线性空间 E 的基为 $\{\beta_i\gamma_j|1\leq i\leq n, 1\leq j\leq m\}$，由于

$$
\begin{aligned}
&\alpha_L(\beta_1\gamma_1,\cdots,\beta_n\gamma_1,\beta_1\gamma_2,\cdots,\beta_n\gamma_2,\cdots\cdots,\beta_1\gamma_m,\cdots,\beta_n\gamma_m)\\
=&(\alpha\beta_1\gamma_1,\cdots,\alpha\beta_n\gamma_1,\alpha\beta_1\gamma_2,\cdots,\alpha\beta_n\gamma_2,\cdots\cdots,\alpha\beta_1\gamma_m,\cdots,\alpha\beta_n\gamma_m)\\
=&\big((\beta_1\gamma_1,\cdots,\beta_n\gamma_1)B,(\beta_1\gamma_2,\cdots,\beta_n\gamma_2)B,\cdots\cdots,(\beta_1\gamma_m,\cdots,\beta_n\gamma_m)B\big)\\
=&(\beta_1\gamma_1,\cdots,\beta_n\gamma_1,\beta_1\gamma_2,\cdots,\beta_n\gamma_2,\cdots\cdots,\beta_1\gamma_m,\cdots,\beta_n\gamma_m)\begin{pmatrix}B&O&\cdots&O\\O&B&\cdots&O\\\vdots&\vdots&\ddots&\vdots\\O&O&\cdots&B\end{pmatrix}_{mn},
\end{aligned}
$$

因此 α_L 在基 $\{\beta_i\gamma_j\}$ 下的矩阵为 mn 阶准对角方阵 $\mathrm{diag}(B,\cdots,B)$，显然它的特征多项式为 f^m.■

推论 70 设 E/F 是有限扩张，$\alpha_1,\cdots,\alpha_n$ 是 $\alpha\in E$ 在 F 上的极小多项式的 n 个根 (注意根的定义 34 中分裂域的条件)，且 $[E:F[\alpha]]=m$，则 $\mathrm{Trace}_{E/F}(\alpha)=m\sum_{i=1}^n\alpha_i,\mathrm{Norm}_{E/F}(\alpha)=(\prod_{i=1}^n\alpha_i)^m$.

证明思路 极小多项式可以写成 $f(x)=\prod(x-\alpha_i)=x^n+a_1x^{n-1}+\cdots+a_n$，其中 $a_1=-\sum\alpha_i,a_n=(-1)^n\prod\alpha_i$. 由命题 69，特征多项式 $\lambda_{E/F}(\alpha,x)=f(x)^m=x^{mn}+ma_1x^{mn-1}+\cdots+a_n^m$. 此时 $\mathrm{Trace}_{E/F}(\alpha)=-ma_1=m\sum\alpha_i,\mathrm{Norm}_{E/F}(\alpha)=(-1)^{mn}a_n^m=(\prod\alpha_i)^m$.■

例 设 E 是 $x^8-2\in\mathbb{Q}[x]$ 的分裂域，可以证明 $[E:\mathbb{Q}]=16$. 注意到 $x^8-2\in\mathbb{Q}[x]$ 是 $\sqrt[8]{2}$ 的极小多项式，$[E:\mathbb{Q}[\sqrt[8]{2}]]=2$，根据线性代数的结论以及命题 69 有：

$\lambda_{\mathbb{Q}[\sqrt[8]{2}]/\mathbb{Q}}(\sqrt[8]{2},x)=$	x^8	$+0x^7$	-2	$\lambda_{E/\mathbb{Q}}(\sqrt[8]{2},x)=(x^8-2)^2=$	x^{16}	$+0x^{15}$	$-4x^8$	$+4$
$\mathrm{Trace}_{\mathbb{Q}[\sqrt[8]{2}]/\mathbb{Q}}(\sqrt[8]{2})=$		0		$\mathrm{Trace}_{E/\mathbb{Q}}(\sqrt[8]{2})=$		0		
$\mathrm{Norm}_{\mathbb{Q}[\sqrt[8]{2}]/\mathbb{Q}}(\sqrt[8]{2})=$			-2	$\mathrm{Norm}_{E/\mathbb{Q}}(\sqrt[8]{2})=$				4.

推论 71 设 E/F 是可分扩张，Ω 是 F 的代数闭包. 记 $\Delta=\{\sigma|F\text{- 同态}\sigma:E\to\Omega\}$，则有 $\mathrm{Trace}_{E/F}(\alpha)=\sum_{\sigma\in\Delta}\sigma(\alpha),\mathrm{Norm}_{E/F}(\alpha)=\prod_{\sigma\in\Delta}\sigma(\alpha)$.

证明思路 当 $E=F[\alpha]$ 时，由命题 17 知 Δ 与 α 的极小多项式 $f\in F[x]$ 在 Ω 中的根一一对应，且 $\sigma(\alpha)$ 正好跑遍 f 的根 ($\sigma\in\Delta$). 此时利用推论 70 即得结论. 考虑一般的 E，由命题 31 知每个 F-同态 $F[\alpha]\to\Omega$ 有 $[E:F[\alpha]]$ 种提升到 E 的方式，因此 f 的每个根出现了 $[E:F[\alpha]]$ 次 (可分性保证无重根). 特别地，我们有推论：当 E/F 是 Galois 扩张时，$\mathrm{Trace}_{E/F}(\alpha)=\sum\limits_{\sigma\in\mathrm{Gal}(E/F)}\sigma(\alpha),\mathrm{Norm}_{E/F}(\alpha)=\prod\limits_{\sigma\in\mathrm{Gal}(E/F)}\sigma(\alpha)$.■

命题 72 设 $F\subseteq M\subseteq E$ 是有限扩张，则有 $\mathrm{Trace}_{M/F}(\cdot)\circ\mathrm{Trace}_{E/M}(\cdot)=\mathrm{Trace}_{E/F}(\cdot)$，$\mathrm{Norm}_{M/F}(\cdot)\circ\mathrm{Norm}_{E/M}(\cdot)=\mathrm{Norm}_{E/F}(\cdot)$.

命题 73 设 $f\in F[x]$ 是首一不可约多项式，α 是 f 的一个根，则 $D(f)=(-1)^{m(m-1)/2}\mathrm{Norm}_{F[\alpha]/F}\big(f'(\alpha)\big)$.

证明思路 由导数的运算法则和推论 71 的证明可知 $D(f)=\prod_{i<j}(\alpha_i-\alpha_j)^2=(-1)^{m(m-1)/2}\prod_i\big(\prod_{j\neq i}(\alpha_i-\alpha_j)\big)=(-1)^{m(m-1)/2}\prod_i f'(\alpha_i)=(-1)^{m(m-1)/2}\prod_\sigma f'\big(\sigma(\alpha)\big)=(-1)^{m(m-1)/2}\mathrm{Norm}_{F[\alpha]/F}\big(f'(\alpha)\big)$.■

命题 74 设 E/F 是有限扩张. 对任意 $\alpha,\beta\in E$ 以及任意 $a,b\in F$，直接计算可得 $\mathrm{Trace}_{E/F}(a\alpha+b\beta)=a\mathrm{Trace}_{E/F}(\alpha)+b\mathrm{Trace}_{E/F}(\beta)$，因此 $\mathrm{Trace}_{E/F}(\cdot):E\to F$ 是线性映射. 此外，它作为 Abel 群同态时只能是满同态或零同态.

推论 75 设 E/F 是有限扩张，则 $\mathrm{Trace}_{E/F}(\cdot):(E,+)\to(F,+)$ 是满同态当且仅当 E/F 可分；是零同态当且仅当 E/F 不可分. 根据命题 40，有限域都是完美的，故当 $E/\mathbb{F}_{p^n}$ 是有限扩张时，$\mathrm{Trace}_{E/\mathbb{F}_{p^n}}(\cdot):(E,+)\to(\mathbb{F}_{p^n},+)$ 是满同态.

► **问题 IV：Galois 上同调和 Kummer 理论** (主要参考文献 [13]Chapter4.3，Chapter6.2)

Kummer 理论是代数数论和类域论的基础. 欲介绍这个理论，首先需要引入 Hilbert90 定理 (定理 79)，它的作用是为了得到某种正合性的结论，借此来推出定理 81(Kummer). 定理 81 断言在某种特殊情况下，区分同构等价的域扩张往往需要依赖于单位根的对称性.

现引入“群上的模”这个概念，读者应注意区分其与“环上的模”这个概念之间的差别.

定义 76(模) 设 G 是一个群，一个 Abel 群 M 配备了一个群 G 在其上的作用 $G\times M\to M,(\sigma,m)\mapsto\sigma(m)$ 之后称为是一个**G-模**，如果这个群作用满足：

(1)$\sigma(m+m')=\sigma(m)+\sigma(m')$，对任意 $\sigma\in G,m,m'\in M$；

(2)$(\sigma\tau)(m)=\sigma(\tau(m))$，对任意 $\sigma,\tau\in G,m\in M$；

(3)$\mathrm{id}(m)=m$，对任意 $m\in M$.

因此，定义 G 在 M 上的作用相当于指定了一个群同态 $G\to\mathrm{End}(M)$. 典范地还可以定义两个 G-模 M、N 之间的同态，它是满足下述条件的映射 $\varphi:M\to N$：

(1)Abel 群同态：$\varphi(m+m')=\varphi(m)+\varphi(m')$，对任意 $m,m'\in M$；

(2) 线性性质：$\varphi(\sigma(m))=\sigma(\varphi(m))$，对任意 $\sigma\in G,m\in M$.

定义 77(主要交叉映射) 设 M 是 G-模. 一个映射 $f:G\to M$ 称为是**交叉**的，如果满足对任意 $\sigma,\tau\in G,f(\sigma\tau)=f(\sigma)+\sigma f(\tau)$. 显然，由 $f(\mathrm{id})=f(\mathrm{id}\cdot\mathrm{id})=f(\mathrm{id})+f(\mathrm{id})$ 可知 $f(\mathrm{id})=0$. 固定 $x\in M$，定义

$h_x : G \to M, \sigma \mapsto \sigma x - x$，可以验证这个映射是交叉映射. 称这样的交叉映射 $h_x(x \in M)$ 为**主要交叉映射**.

设 M 是 G-模. 可以验证所有交叉映射构成一个 Abel 群，记为 $\mathrm{Cross}(G, M)$；所有主要交叉映射也构成一个 Abel 群，记为 $\mathrm{Principal}(G, M) \subseteq \mathrm{Cross}(G, M)$. 约定这些记号后，定义**第 1 维上同调群**为 $H^1(G, M) = \{\mathrm{Cross}(G, M)\}/\{\mathrm{Principal}(G, M)\}$. 当然可以定义更高维的上同调，但这里只需用到第 1 维上同调即可.

定理 78(长正合列定理) 设有 G- 模的正合列 $0 \to M' \to M \to M'' \to 0$，则可导出 Abel 群的长正合列 $1 \to M'^G \to M^G \to M''^G \xrightarrow{\partial} H^1(G, M') \to H^1(G, M) \to H^1(G, M'')$. 其中 $M^G = \{x \in M | \forall \sigma \in G, \sigma(x) = x\}$. 这里 ∂ 称为**连接同态**，它由同调代数基本定理给出. 用抽象废话的语言来说，函子 $\square^G : \mathbf{Mod}(G) \to \mathbf{AbGroup}, M \mapsto M^G$ 是左正合共变函子 (具体同调代数的理论还请参考 [12]).

定理 79(Hilbert90) 设 E/F 是有限循环扩张，记 $\mathrm{Gal}(E/F) = \langle\sigma\rangle$. 又设 $\alpha \in E^\times$，若 $\mathrm{Norm}_{E/F}(\alpha) = 1$，则存在 $\beta \in E$，使得 $\alpha = \beta/\sigma(\beta)$.

定义 80(指数) 称群 G 具有**指数**n，如果对任意 $\sigma \in G$，$\sigma^n = \mathrm{id}$(n 是最小的满足这一条件的正整数).

例 根据 Abel 群的结构定理，指数为 n 的有限 Abel 群必然同构于 $\bigoplus_r \mathbb{Z}/n\mathbb{Z}$ 的某个子群，$r \geq 1$.

设 F 是域，$1 \neq \zeta$ 是 n 次本原单位根$\big(\mathrm{Char}(F) \nmid n\big)$. 又设 E/F 是有限 Galois 扩张，则有乘法 Abel 群的短正合列 (下面的叙述混淆 1 和 0，因为模正合列首先得是 Abel 群正合列)

$$0 \longrightarrow \mu_n \longrightarrow (E^\times, \cdot) \xrightarrow{x \mapsto x^n} \big((E^\times)^n, \cdot\big) \longrightarrow 0\,,$$

其中 $\mu_n = \{\zeta \in E | \zeta^n = 1 \in F\}$，$(E^\times)^n = \{x^n | x \in E^\times\}$. 可以把上述正合列看成是关于 $\mathrm{Gal}(E/F)$-模的正合列，蕴含的群作用即为熟知的 F- 同态. 将函子 $\square^{\mathrm{Gal}(E/F)}$ 作用其上并应用 Hilbert90 定理 79 得到长正合列$\big(H^1(\mathrm{Gal}(E/F), E^\times) = 1$ 的证明见 [13] 命题 4.3.8$\big)$

$$1 \longrightarrow \mu_n \longrightarrow F^\times \xrightarrow{x \mapsto x^n} (E^\times)^n \cap F^\times \longrightarrow H^1(\mathrm{Gal}(E/F), \mu_n) \longrightarrow 1.$$

利用上面的陈述，我们可以证明以下定理 (证明略)：

定理 81(Kummer) 设 E/F 是有限 Galois 扩张，$1 \neq \zeta \in E$ 是 n 次本原单位根$\big(\mathrm{Char}(F) \nmid n\big)$. 指定 F 的某一个代数闭包 Ω，此时存在集合之间的一一对应：

$$\begin{aligned} \{F\text{包含在 } \Omega \text{ 中且对应 Galois 群指数为 } n \text{ 的有限 Abel 扩张}\} &\longleftrightarrow \{F^\times/(F^\times)^n\text{的有限子群 } B\} \\ E &\longrightarrow (E^\times)^n \cap F^\times \\ \bigcap_L \{L | F[b^{\frac{1}{n}}] \subseteq L \subseteq \Omega, \forall b \in B\} = F[B^{\frac{1}{n}}] &\longleftarrow B. \end{aligned}$$

特别地，如果 $E \leftrightarrow B$，则 $[E : F] = (B : (F^\times)^n)$.

例 $\{\mathbb{R}$ 的二次扩张$\} \longleftrightarrow \{\mathbb{R}^\times/(\mathbb{R}^\times)^2 \cong (\{\pm 1\}, \times)$ 的有限子群$\}$.

▶ **问题 V：Riemann 曲面的覆叠和亚纯函数域** (主要参考文献 [4]Chapter1.8 和 [7]Chapter11.2)

Galois 对应的精妙绝不仅体现在单纯的解代数方程上，它在代数拓扑中也是有联系的. 下面提供一个建立在 Riemann 曲面理论上的例子，其中涉及到的函数均是复变函数. 记号 $\mathcal{O}_X$ 指 Riemann 曲面 X 上的全纯函数环 (层)，$\mathcal{M}_X$ 指 X 上的亚纯函数域 (层). 注意 $\mathcal{M}_X = \mathrm{frac}(\mathcal{O}_X)$.

定义 82(预备知识) 称函数 $w = w(z)$ 为**代数函数**，如果它满足某个系数在域 $\mathcal{M}_X$ 中的方程 $w^n + f_1(z)w^{n-1} + \cdots + f_n(z) = 0$，其中 X 是 Riemann 曲面.

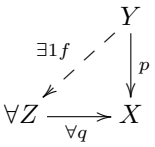
设 X, Y 是拓扑空间，$p : Y \to X$ 是连续映射. 对于 $x \in X$，称集合 $p^{-1}(x)$ 为映射 p **在** x **上的纤维**. 如果 $p : Y \to X$ 和 $q : Z \to X$ 均连续，映射 $f : Y \to Z$ 称为**保纤维**的，如果 $p = q \circ f$. 这意味着 $x \in X$ 的纤维被映入 x 的纤维.

设 X, Y 是 Hausdorff 的拓扑空间，映射 $p : Y \to X$ 称为**覆叠映射**，如果任意 $x \in X$ 以某个 U 为开邻域，均有 $p^{-1}(U) = \bigcup_{i \in I} V_i$，其中 V_i 是 Y 中互不相交的开子集，且所有的 $p|_{V_i} : V_i \to U$ 均是同胚. 此时 Y 称为 X 的**覆叠空间**. 可以证明，当 X 道路连通时，任意 $x_1, x_2 \in X$，必有势 $|p^{-1}(x_1)| = |p^{-1}(x_2)|$，因此可以定义

覆叠映射 p 的**叶数**为势 $|p^{-1}(x)|$，这里 $x\in X$. 此外，覆叠映射 p 是一个局部同胚，如果 $Y\neq\varnothing$，则 p 是满的.

设 X,Y 是 Riemann 曲面，$p:Y\to X$ 是非常值全纯映射. 一个点 $y\in Y$ 称为 p 的**分歧点**，如果不存在 y 的邻域 V 使得 $p|_V$ 是单射. 若 p 有 (无) 分歧点，则称 p 是**分歧 (无支) 全纯映射**. 特别，若一个映射除去分歧点之后是覆叠映射，则称其为**分歧覆叠映射**.

设 X,Y 是连通拓扑空间，$p:Y\to X$ 是覆叠映射. 称 p 为 X 的**万有覆叠** (有时也将 Y 称为 X 的万有覆叠)，如果满足泛性质：对任意覆叠映射 $q:Z\to X(Z$ 连通) 及任意选取 $y_0\in Y$ 与 $z_0\in Z$ 使得 $p(y_0)=q(z_0)$，总存在唯一保纤维映射 $f:Y\to Z$，使得 $f(y_0)=z_0$. 即下图可交换：



可以证明，万有覆叠在同胚的意义下唯一. 另外，还可以证明，$p:Y\to X$ 是万有覆叠当且仅当 p 是覆叠映射且 Y 是单连通的.

设 X,Y 是拓扑空间，$p:Y\to X$ 是覆叠映射. 该覆叠映射的一个**覆叠变换**是指一个保纤维同胚 $f:Y\to Y$. 可以验证在此前提下所有的覆叠变换关于复合作成一个群，称为**覆叠变换群**，记作 $\mathrm{Deck}(Y/X)$.

设 X,Y 是连通 Hausdorff 拓扑空间，覆叠映射 $p:Y\to X$ 称为是 **Galois**的，如果任意 $y_0,y_1\in Y$ 满足 $p(y_0)=p(y_1)$，总存在覆叠变换 $f:Y\to Y$，使得 $f(y_0)=y_1$(这里 f 的选取与 y_0,y_1 有关).

定理 83 设 X 是 Riemann 曲面，$p(T)=T^n+c_1T^{n-1}+\cdots+c_n\in\mathcal{M}_X[T]$ 是不可约多项式，则存在一个三元组 (Y,π,F)：Y 是一个 Riemann 曲面、$\pi:Y\to X$ 是一个分歧全纯 n-叶覆叠映射以及 $F\in\mathcal{M}_Y$ 是一个亚纯函数，满足 $F^n+(\pi^*c_1)F^{n-1}+\cdots+\pi^*c_n=0$，其中 $\pi^*:\mathcal{M}_X\to\mathcal{M}_Y,f\mapsto f\circ\pi$. 此外，若三元组 (Z,τ,G) 也满足上述性质，则存在唯一的保纤维双全纯映射 $\sigma:Z\to Y$，使得 $G=F\circ\sigma$. 这里的三元组 (Y,π,F) 或其中的 F 称为由多项式 $p(T)$ 决定的代数函数.

定理 84 设 X 是 Riemann 曲面，$p(T)\in\mathcal{M}_X[T]$ 为首一不可约 n 次多项式. 由定理 83，存在三元组 (Y,π,F)，其中 F 是一个代数函数. 此时 $\pi^*:\mathcal{M}_X\hookrightarrow\mathcal{M}_Y,f\mapsto f\circ\pi$ 是一个次数为 n 的域扩张，且 $\mathcal{M}_Y\cong\mathcal{M}_X[T]/(p(T))$. 此外，每个覆叠变换 $\sigma:Y\to Y$ 诱导 $\mathcal{M}_Y$ 的 $\mathcal{M}_X$-自同构 $\bar\sigma:\mathcal{M}_Y\to\mathcal{M}_Y,f\mapsto f\circ\sigma^{-1}$，因此有群同构 $\mathrm{Deck}(Y/X)\xrightarrow{\sim}\mathrm{Aut}(\mathcal{M}_Y/\mathcal{M}_X)$. 特别，$\mathcal{M}_Y/\mathcal{M}_X$ 是 Galois 扩张当且仅当覆叠 $\pi:Y\to X$ 是 Galois 的.

定理 85(覆叠 Galois 基本定理) 设 $\mathcal{M}_Y/\mathcal{M}_X$ 是由 n 次首一不可约多项式 $p(T)\in\mathcal{M}_X[T]$ 决定的 Galois 扩张，则存在一一对应：

$$\{\mathrm{Deck}(Y/X)\text{的子群}\}\longleftrightarrow\{\mathcal{M}_Y/\mathcal{M}_X\text{的中间亚纯函数域}\}.$$

由于 $\mathcal{M}_Y/\mathcal{M}_X$ 是次数为 n 的域扩张，因此 $|\mathrm{Deck}(Y/X)|<\infty$.

► **问题 VI：线性微分方程的 Picard-Vessiot 理论** (主要参考文献 [6]、[7]Chapter11.1、[8]Chapter1.5 和 [9])

Picard-Vessiot 理论发展于 20 世纪前后，它的主要结果大致是说，一个线性微分方程 (组) “可通过积分求解”当且仅当它的微分 Galois 群是连通且可解的. 不过原论文并没有精确地定义何为“可通过积分求解”，这部分工作是 Kolchin 在 20 世纪完善的，他给出了精确的定义以及一系列算法，并且还作了一些推广，开辟了微分代数这门学科. 本节的目的是粗略地介绍 Picard-Vessiot 理论.

定义 86(微分域和 P.-V. 扩张) 一个**微分域**(一般为函数域，例如 $\mathbb{C}(x)$)$K=(K,\partial)$ 是一个域且配备了一个导数算子 $\partial:K\to K$，记为 $\partial a=a',\partial^k a=a^{(k)}$，它满足 Leibnitz 律：$\partial(a+b)=\partial a+\partial b,\partial(ab)=\partial(a)b+a\partial(b)$. 推广地，域 K 配备了满足 Leibnitz 律的导数算子组 $\Delta=\{\partial_1,\cdots,\partial_r\}$ 后亦可称 (K,Δ) 为微分域. 类似地可定义微分环或微分理想. 微分域 (环) 之间的**同态**首先是代数意义上的域 (环) 同态，且与导数算子 ∂ 可交换. 微分域 (K,∂) 的子域 $\mathcal{C}_K$ 称为 K **的常数域**，如果 $\mathcal{C}_K$ 由所有满足 $\partial u=0$ 的那些 u 组成. 例如 $\mathcal{C}_{(\mathbb{C}(x),\frac{d}{dx})}=\mathbb{C}$.

设 $K\subseteq\widetilde{K}$ 是微分域，$u\in\widetilde{K}\setminus K$. 仿照经典的扩域理论，我们定义$K$ **添加** u **的域扩张**为 $K\langle u\rangle=$

$K(u,u',u'',\cdots)\subseteq\widetilde{K}$. 这里扩张 $K\langle u\rangle/K$ 可有限可超越. 设 $D=\partial^n+a_{n-1}\partial^{n-1}+\cdots+a_0(a_i\in K)$ 为一个 n 阶线性导数算子，令 $y_1,\cdots,y_n$ 为微分方程 $Dy=0$ 解空间的一组基. 考虑添加 $y_1,\cdots,y_n$ 的域扩张 $K\langle y_1,\cdots,y_n\rangle/K$，称它是 K **关于方程** $Dy=0$ **的 Picard-Vessiot 扩张** (注意 Picard-Vessiot 扩张依赖方程 $Dy=0$，不需要强调该方程时可简称其为 P.-V. 扩张)，如果满足：

(1) 域 $K\langle y_1\cdots,y_n\rangle$ 不含新的使 $\partial u=0$ 的 u，即 $\mathcal{C}_{K\langle y_1\cdots,y_n\rangle}=\mathcal{C}_K$；

(2)$y_1\cdots,y_n$ 在 $\mathcal{C}_K$ 上线性无关，即 Wronski 行列式

$$\mathcal{W}=W(y_1\cdots,y_n)=\begin{vmatrix} y_1 & y_2 & \cdots & y_n \\ y_1' & y_2' & \cdots & y_n' \\ \cdots & \cdots & \ddots & \cdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{vmatrix}\neq 0.$$

定义 87(微分 Galois 群) 设 M/K 是 P.-V. 扩张. 称微分域 M 的所有保持 K 不动的自同构组成的群为 M/K 的**微分 Galois 群**，记为 $\mathrm{DGal}(M/K)$. 特别，定义 86 中微分方程 $Dy=0$ 的微分 Galois 群定义为 $\mathrm{DGal}(K\langle y_1\cdots,y_n\rangle/K)$. 可以证明这里的微分 Galois 群是 $GL(n,\mathcal{C}_K)$ 的子群 (见定理 89.3，这里 $\mathcal{C}_K$ 一般为 $\mathbb{C}$). 此外，微分 Galois 群是代数群，其上含有自然的 Zariski 拓扑 (看成代数几何意义下的代数簇).

注意 以解微分方程为目的，定义 87 中的 K 一般取为 $\mathbb{C}(x)$，然后考虑其上的微分域扩张.

例 线性常微分方程 $\frac{dy}{dx}+2xy=0$ 的通解为 $y=Ce^{-x^2}$，$u=e^{-x^2}$ 是基. 易证 $\mathbb{C}(x)\langle u\rangle=\mathbb{C}(x,u,u',\cdots)\cong\mathbb{C}(x,e^{-x^2})$. 此时该方程的微分 Galois 群为可解群 $\mathrm{DGal}\big(\mathbb{C}(x,e^{-x^2})/\mathbb{C}(x)\big)\cong\mathbb{C}^\times$.

定理 88(P.-V. 扩张的存在唯一性) 设 (K,∂) 是微分域，D 是系数在 K 中的一个线性微分算子，则存在 K 关于方程 $Dy=0$ 的 P.-V. 扩张，且此扩张在同构的意义下唯一.

定理 89(Kolchin) (1) 设 M/K 是 P.-V. 扩张，令 $x\in M\backslash K$，此时存在 $\sigma\in\mathrm{DGal}(M/K)$ 使得 $\sigma(x)\neq x$.

(2) 设 $K\subseteq L\subseteq M$ 是微分域，其中 L/K 及 M/K 是 P.-V. 扩张，则任意 $\sigma\in\mathrm{DGal}(L/K)$ 均可提升为 M 的一个自同构.

(3) 若 M/K 是 (关于 $Dy=0$ 的)P.-V. 扩张，则 $\mathrm{DGal}(M/K)$ 与 $GL(n,\mathcal{C}_K)$ 的某个子群同构. 这里 n 为 $Dy=0$ 解空间的维数.

(4) 设 $K\subseteq L\subseteq M$ 是微分域，其中 M/K 是 P.-V. 扩张，则 (i)M/L 也是 P.-V. 扩张；(ii)L/K 是 P.-V. 扩张当且仅当 $H=\mathrm{DGal}(M/L)$ 是 $G=\mathrm{DGal}(M/K)$ 的正规子群. 此时 $\mathrm{DGal}(L/K)\cong G/H$.

定理 90(微分 Galois 基本定理) 设 M/K 是 P.-V. 扩张，$G=\mathrm{DGal}(M/K)$，则存在一一对应：

$$\begin{aligned}\{G\text{的 Zariski 闭子群 (代数子群)}\}&\longleftrightarrow\{M/K\text{的中间微分域}\}\\ H&\longrightarrow M^H\\ \mathrm{DGal}(M/L)&\longleftarrow L.\end{aligned}$$

定义 91(广义 Liouville 扩张) 称 P.-V. 扩张 M/K 是 **Liouville 扩张**，如果存在微分域塔 $K=K_0\subseteq\cdots\subseteq K_r=M$，使得每个扩张 K_{i+1}/K_i 只能由如下两种方式之一得到：(1)$K_{i+1}=K_i\langle u\rangle$，其中 $u'=a\in K_i$；(2)$K_{i+1}=K_i\langle v\rangle$，其中 $v'=av,a\in K_i$. 当 $K=\mathbb{C}(x)$ 时，任意 Liouville 扩张 $M/\mathbb{C}(x)$ 中的函数称为**可积分表示的**. 称 P.-V. 扩张 M/K 是**广义 Liouville 扩张**，如果存在微分域塔 $K=K_0\subseteq\cdots\subseteq K_r=M$，使得每个扩张 K_{i+1}/K_i 只能由如下三种方式之一得到：(1)$K_{i+1}=K_i\langle u\rangle$，其中 $u'=a\in K_i$；(2)$K_{i+1}=K_i\langle v\rangle$，其中 $v'=av,a\in K_i$；(3)$K_{i+1}=K_i[\alpha]$，其中 α 是代数元. 当 $K=\mathbb{C}(x)$ 时，任意广义 Liouville 扩张 $M/\mathbb{C}(x)$ 中的函数称为**可广义积分表示的**.

现在给出主要定理：

定理 92 一个 P.-V. 扩张 M/K 是 Liouville 扩张当且仅当它的微分 Galois 群可解；一个 P.-V. 扩张 M/K 是广义 Liouville 扩张当且仅当它的微分 Galois 群中 id 的连通分支是可解群.

4、无穷 Galois 扩张与超越扩张

定义 93(无穷 Galois 扩张) E/F 称为是 **Galois 扩张**，如果 E/F 是可分正规的代数扩张. 对应的 Galois 群仍记为 $\mathrm{Gal}(E/F)$. 例如 $\mathbb{A}/\mathbb{Q}$ 就是一个 (无穷)Galois 扩张.

之前我们只给出了扩张次数有限情形下的 Galois 对应 (定理 51). 本节的目标是建立无穷扩张情形下的 Galois 对应 (定理 98)，事实上此时的 Galois 群带有一个典范的拓扑结构 (即它是拓扑群).

定义 94(拓扑群) **拓扑群**即群 G 上又配备了一个拓扑结构 $\mathcal{T}$，使得 $(G\times G, \text{积拓扑}) \to (G,\mathcal{T}), (g,h)\mapsto gh$ 和 $(G,\mathcal{T})\to(G,\mathcal{T}), g\mapsto g^{-1}$ 均连续. 一般将 $(G,\mathcal{T})$ 简记为 G.

注意 设 G 是拓扑群，$a\in G$. 此时可定义**左平移同胚**$a_L: G\to G, g\mapsto ag$. 由于它是复合映射 $G\to G\times G\to G, g\mapsto (a,g)\mapsto ag$，故连续. 事实上 $(a_L)^{-1}=(a^{-1})_L$. 类似地可以定义右平移同胚. 因此，对任意子群 $H\subseteq G$，陪集 aH 开 (闭) 当且仅当 H 开 (闭). 此外，注意到 $G\backslash H=\bigcup_{g\notin H} gH$(读者自证)，故 H 开 $\Rightarrow H$ 闭；H 闭且 $(G:H)<\infty\Rightarrow H$ 开.

我们先给出一个简单的命题，这个命题将启发我们如何给 Galois 群赋予拓扑结构.

命题 95 设 E/F 是 (无穷)Galois 扩张，若记 $\mathcal{G}=\{\text{Galois 群}\,\mathrm{Gal}(E/L)|F\subseteq L\subseteq E, [L:F]<\infty\}$ 为 $\mathrm{Gal}(E/F)$ 的子群构成的集合，此时有：

(1)$\bigcap_{H\in\mathcal{G}} H=\{\mathrm{id}\}$.

(2)$\mathcal{G}$ 对有限交封闭.

(3) 任意 $H\in\mathcal{G}$ 均包含了 $\mathrm{Gal}(E/F)$ 的一个正规子群 $N\in\mathcal{G}$.

(4) 对任意 $H\in\mathcal{G}$，$\big(\mathrm{Gal}(E/F):H\big)<\infty$.

定义 96(Krull 拓扑) 设 E/F 是 (无穷)Galois 扩张. 记 $\mathcal{N}$ 为 $\mathcal{G}$ 中所有正规子群 N 的陪集构成的集合；$\mathcal{L}$ 为 $\mathcal{G}$ 中所有子群 H 的左陪集构成的集合；$\mathcal{R}$ 为 $\mathcal{G}$ 中所有子群 H 的右陪集构成的集合. 此时 $\mathcal{N}$ 可构成 $\mathrm{Gal}(E/F)$ 的一个拓扑基 (也可以用 $\mathcal{L}$ 和 $\mathcal{R}$ 生成)，其生成的拓扑称为 **Krull 拓扑**. 具体来说，这个拓扑里面的开集是若干个 $\mathcal{N}$ 中元素的并 (或若干个 $\mathcal{L}$ 中元素的并，或若干个 $\mathcal{R}$ 中元素的并). 由上面的注意和命题 95(4)，显然每个子群 $H\in\mathcal{G}$(及其陪集) 在这个拓扑下都是既开又闭的.

特别，当 $\mathrm{Gal}(E/F)$ 是有限群的时候，不难验证此时单点集 $\{\mathrm{id}\}$ 是开集且 Krull 拓扑是离散拓扑. 此外，还可以证明，如果中间域 L/F 是有限的 Galois 扩张，那么限制映射 $p_L:\mathrm{Gal}(E/F)\to\mathrm{Gal}(L/F), \sigma\mapsto\sigma|_L$ 是连续的 (证明见 [1] 命题 7.7，此时 $\mathrm{Gal}(L/F)$ 上的拓扑是离散拓扑).

注意 关于无穷 Galois 扩张，也有与有限的情况类似的性质 (还有些性质依赖于 Galois 群的拓扑性质)，例如：

(1) 若 E/F 是无穷 Galois 扩张，则对任意中间域 $F\subseteq L\subseteq E$，有：(i)E/L 是 Galois 扩张，(ii) 任意 F-同态 $\varphi: L\to E$ 均可提升为 F- 同构 $\bar{\varphi}: E\to E$(即 $\bar{\varphi}|_L=\varphi$)；

(2)E/F 是无穷 Galois 扩张当且仅当 $[E:F]=\infty$ 且 $E^{\mathrm{Aut}(E/F)}=F$；

等等. 更一般地，有如下命题描述了无穷 Galois 群上 Krull 拓扑的性质：

命题 97 配备了 Krull 拓扑的 $\mathrm{Gal}(E/F)$ 是紧 Hausdorff 且完全不连通的 (若对拓扑空间 X 中的任意两点 $x\neq y$，总存在开集 U,V，使 $x\in U, y\in V$ 且 $U\cap V=\varnothing, U\cup V=X$，则称拓扑空间 X 为**完全不连通空间**).

证明思路 Hausdorff：对 $\sigma,\tau\in\mathrm{Gal}(E/F), \sigma\neq\tau$，由于 $\bigcap_{H\in\mathcal{G}} H=\{\mathrm{id}\}$，必存在 $H\in\mathcal{G}$，$\sigma^{-1}\tau\notin H$. 此时 σH 与 τH 不交. 完全不连通：注意到 $\sigma\in\sigma H$ 以及 $\tau\in\mathrm{Gal}(E/F)\setminus\sigma H$ 即可. 紧：这是 Tychonoff 定理的一个应用，详细证明见 [14] 命题 5.4.4.■

定理 98(Krull) 设 E/F 是 (无穷)Galois 扩张，则存在一一对应：

$$\begin{aligned}\{\mathrm{Gal}(E/F)\text{的闭子群}\} &\longleftrightarrow \{E/F\text{的中间域}\}\\ H &\longrightarrow E^H\\ \mathrm{Gal}(E/L) &\longleftarrow L.\end{aligned}$$

此外，还有：

(1) 上述对应满足 $H_1\supseteq H_2\Leftrightarrow E^{H_1}\subseteq E^{H_2}$(反变).

(2)$\mathrm{Gal}(E/F)$ 的闭子群 H 开当且仅当 E^H/F 是有限扩张. 此时还有 $\big(\mathrm{Gal}(E/F):H\big)=[E^H:F]$.

(3) 对任意 $\sigma\in\mathrm{Gal}(E/F)$，$E^{\sigma H\sigma^{-1}}=\sigma(E^H),\mathrm{Gal}(E/\sigma L)=\sigma\,\mathrm{Gal}(E/L)\sigma^{-1}$.

(4)$\mathrm{Gal}(E/F)$ 的闭子群 H 正规 $\Leftrightarrow E^H/F$ 是 Galois 扩张 (可以无穷). 此时商群 $\mathrm{Gal}(E/F)\big/H\cong\mathrm{Gal}(E^H/F)$.

(5) 一般地，如果 H 是 $\mathrm{Gal}(E/F)$ 的子群 (不一定闭)，那么 E/E^H 是 (无穷)Galois 扩张，且 $\mathrm{Gal}(E/E^H)$ 等于 H 在 $\mathrm{Gal}(E/F)$ 中的闭包.

注意 定理 51 是定理 98 的推论：当 $[E:F]<\infty$ 时，$\mathrm{Gal}(E/F)$ 上的 Krull 拓扑是离散拓扑，因此它的所有子群当然都是闭的.

注意 (这里的术语可参考 [12]Chapter5.2) 我们也可以用范畴论的语言来描述如何构造无穷扩张的 Galois 群，这得益于 Krull 拓扑从纯拓扑的角度来看是一类比较特殊的拓扑. 设 E/F 是无穷 Galois 扩张，考虑有限群的反向系统

$$\big\{\{\mathrm{Gal}(L/F)\}_{[L:F]<\infty}\ ,\ p_L^{L'}:\mathrm{Gal}(L'/F)\to\mathrm{Gal}(L/F)\big\},$$

其反向极限在群范畴中存在并且就是

$$\big(\mathrm{Gal}(E/F)\ ,\ p_L:\mathrm{Gal}(E/F)\to\mathrm{Gal}(L/F)\big),$$

这里 p_L 是之前给出的连续限制映射，在反向极限中称之为投射. 上式或写成 $\varprojlim\mathrm{Gal}(L/F)\cong\mathrm{Gal}(E/F)$，这也是拓扑群的同构.

作为无穷 Galois 扩张的一个例子，接下来我们介绍超越扩张及其相应版本的“Galois”对应.

定义 99(代数相关性) 设 E/F 是 (一般的) 域扩张，$A=\{\alpha_1,\cdots,\alpha_n\}\subseteq E$. 集合 A 给出了一个 F-同态 $\varphi:F[x_1,\cdots,x_n]\to E,f\mapsto f(\alpha_1,\cdots,\alpha_n)$. 如果 $\ker\varphi=(0)$，则称 A(或具体地，这些 α_i) 在 F 上**代数无关**，否则称为在 F 上**代数相关**. 换句话说，这些 α_i 在 F 上代数相关当且仅当存在非零多项式 $f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$ 使得 $f(\alpha_1,\cdots,\alpha_n)=0$. 称无限集 A 在 F 上**代数无关**，如果 A 的任意有限子集在 F 上代数无关，否则称 A 在 F 上**代数相关**. 由定义，如果 $A=\{\alpha_1,\cdots,\alpha_n\}$ 在 F 上代数无关，则有单同态 $\widetilde{\varphi}:F[x_1,\cdots,x_n]\to F[\alpha_1,\cdots,\alpha_n],f(x_1,\cdots,x_n)\mapsto f(\alpha_1,\cdots,\alpha_n)$. 显然这里的 $\widetilde{\varphi}$ 还是同构. 取分式域得同构 $\mathrm{frac}(\widetilde{\varphi}):F(x_1,\cdots,x_n)\xrightarrow{\sim}F(\alpha_1,\cdots,\alpha_n),x_i\mapsto\alpha_i$. 称得到的 $F(\alpha_1,\cdots,\alpha_n)$ 是 F 的**纯超越扩张** (即代数无关蕴含纯超越扩张).

注意 代数相关性这个概念是线性相关性的推广，判断线性相关性时取 f 为一次多项式.

例 显然，一个元素 α 在 F 上代数无关当且仅当它在 F 上超越；而对有限代数扩张 $F[\alpha_1,\cdots,\alpha_n]/F$ 而言，这些 α_i 都是代数相关的. 我们指出 $\{\sqrt{2},\pi,e\}$ 在 $\mathbb{Q}$ 上代数无关，但证明并不容易.

定理 100 设 E/F 是代数扩张，$A=\{\alpha_1,\cdots,\alpha_m\}$，$B=\{\beta_1,\cdots,\beta_n\}$ 是 E 的两个子集. 若 A 在 F 上代数无关，在 $F(B)$ 上代数相关，则 $m\le n$(在线性代数中理解为 A 可以被 B 表出).

定义 101(超越基) 设 E/F 是域扩张.E 在 F 上的**超越基**是一个代数无关集 A，使得 E 在 $F(A)$ 上代数.

引理 102 设 E/F 是域扩张. 使 $E/F(A)$ 是代数扩张的最小的那个集合 $A\subseteq E$ 就是 E 在 F 上的超越基.

证明思路 反证法. 如果这个最小的集合 A 在 F 上不是代数无关的，则存在 $\alpha\in A$ 在 $F(A\setminus\{\alpha\})$ 上代数相关，即 α 或 $F(A)$ 在 $F(A\setminus\{\alpha\})$ 上代数. 根据推论 19(2)，E 在 $F(A\setminus\{\alpha\})$ 上代数，与 A 的最小性矛盾.■

由引理 102 可以直接推出如下定理：

定理 + 定义 103 设 E/F 是域扩张. 如果存在有限子集 $A\subseteq E$ 使得 $E/F(A)$ 是代数扩张，则 E 在 F 上一定存在一个有限超越基. 此外，若还有其它超越基，那么它们的势必定相等. 这个势就称为是域扩张 E/F 的**超越维数**.

例 以紧复流形为例：

(1)Riemann 球面 $\mathbb{CP}^1$ 上的亚纯函数域是 $\mathbb{C}(z)$. 此时 $\mathbb{C}(z)/\mathbb{C}$ 是超越维数为 1 的纯超越扩张.

(2) 复环面 $\mathbb{C}/(\mathbb{Z}\oplus\mathrm{i}\mathbb{Z})$ 上的亚纯函数域是 $\mathbb{C}(\wp,\wp')$，其中 $\wp$ 指亚纯的 Weierstrass 函数 $\wp(z)=\frac{1}{z^2}+\sum_{n^2+m^2\neq0}\big(\frac{1}{(z-n-m\,\mathrm{i})^2}-\frac{1}{(n+m\,\mathrm{i})^2}\big)$，并且它还满足常微分方程 $\wp'(z)^2=4\wp(z)^3-60G_4(z)\wp(z)-140G_6(z)$，其中 G_4,G_6 分别是权为 $4,6$ 的 Eisenstein 级数 (全纯的非尖点形式，见 [15]).

定理 104 设 $\Omega,\Omega'\supseteq F$ 是代数闭域，且 Ω/F 的超越维数等于 Ω'/F 的超越维数，则存在 F-同构 $\Omega\xrightarrow{\sim}\Omega'$.

作为本节的结束，下面我们给出超越扩张情形下的“Galois”对应.

定理 105 设 E/F 是域扩张，且 $E^{\mathrm{Aut}(E/F)}=F$. 可以按命题 95、定义 96 类似的办法给 $\mathrm{Aut}(E/F)$ 赋予 Krull 拓扑(更直接地，对任意 E 的有限子集 S，令 $G(S)=\{\sigma\in\mathrm{Aut}(E/F)|\forall s\in S,\sigma s=s\}$，可以验证 $G(S)$ 是 $\mathrm{Aut}(E/F)$ 的子群，它构成的邻域基结构可以生成 $\mathrm{Aut}(E/F)$ 的一个拓扑)，此时有 (注意，超越扩张不是代数扩张，因而也不可能是 Galois 扩张，但这不影响我们得到类似的结论)：

(1) 对任意有限扩张 $L/F, L\subseteq E$，均有 $E^{\mathrm{Aut}(E/L)}=L$.

(2) 存在一一对应：

$$\begin{aligned}\{\mathrm{Aut}(E/F)\text{的紧子群}\}&\longleftrightarrow\{L|F\subseteq L\overset{\text{Galois}}{\subseteq}E\}\\ H&\longrightarrow E^H\\ \mathrm{Aut}(E/L)&\longleftarrow L.\end{aligned}$$

(3) 如果存在 F 上有限生成的域 L，使得 E/L 是 Galois 扩张，那么 $\mathrm{Aut}(E/F)$ 是局部紧的，且：

$$\begin{aligned}\{\mathrm{Aut}(E/F)\text{的开紧子群}\}&\longleftrightarrow\{L|F\overset{\text{有限生成}}{\subseteq}L\overset{\text{Galois}}{\subseteq}E\}\\ H&\longrightarrow E^H\\ \mathrm{Aut}(E/L)&\longleftarrow L.\end{aligned}$$

(4) 设 H 是 $\mathrm{Aut}(E/F)$ 的子群，$L=E^H$. 则 L 的代数闭包 $\overline{L}$ 在 L 上是 Galois 扩张. 此外，若成立 $H=\mathrm{Aut}(E/L)$，则 $\mathrm{Aut}(E/\overline{L})$ 是 H 的正规子群，且 $H\big/\mathrm{Aut}(E/\overline{L})$ 同构于 $\mathrm{Aut}(\overline{L}/L)$ 的某个稠密子群 (具体的同构映射即限制 $\sigma\mapsto\sigma|_{\overline{L}}$).

从这里开始，代数数论和自守函数理论拉开了序幕，而 Galois 理论的介绍则告一段落.