有限群表示论

●曹锡华　时俭益

●高等教育出版社

有限群表示论

曹锡华　时俭益

高等教育出版社

(京)112号

内 容 简 介

本书旨在介绍有限群的常表示理论，即有限群在特征数不整除群的阶数的域上的表示理论。其中包括群表示论的基本概念与二条主要研究途径的介绍，并着重论述了与群的诱导表示有关的一些经典结果，同时也探讨了域的选取与群表示分解之间的关系。本书为求自成系统，在第一章用较大篇幅简要地叙述了与群表示论有关的一些预备知识，特别是介绍了有限维代数结构与表示理论。本书每节后都附有足够多的习题帮助读者理解与拓广正文的内容。

本书假定读者已经熟悉线性代数理论，并具备群论，环论与域的伽罗华理论方面的最基本知识。本书可作为研究生与高年级本科生的教科书，也可供有关专业的数学工作者与高校教师阅读。

有限群表示论

曹锡华　时俭益

*

高等教育出版社出版

新华书店总店北京科技发行所发行

高等教育出版社激光照排技术部照排

高等教育出版社印刷厂印装

*

开本 850×1168　1/32　印张 8　字数 200 000

1992 年 10 月第 1 版　1992 年 10 月第 1 次印刷

印数 0 001—1 693

ISBN7—04—003876—5/D・1135

定价：3.50 元

前　言

群表示理论是近代数学中发展迅速且相当活跃的数学分支，它包括群的常表示理论，模表示理论与整表示理论，其中，有限群的常表示理论创立最早，迄今已有一百年左右历史，发展也最完善，是研究其它群的表示理论的基础.

群表示理论是在线性代数、群论、环论、域的伽罗华理论、代数结构理论、模论与代数数论等数学学科的基础上发展起来的. 随之群表示理论又与更多的数学学科发生了互相联系，它与范畴论，代数 K 理论，代数几何等学科的关系日趋密切，且从这些学科中不断汲取新的方法并充实新的内容. 同时它也被广泛地应用于其它学科，一些较早期的如 Burnside 的群可解性等问题与较新的如有限单群分类等问题的解决都得力于群的表示理论.除此以外，群表示理论在物理、化学、天文学与建筑学等一些自然科学与科技领域里也有广泛的应用.

有限群的常表示理论是群在特征数不整除群的阶数的域上的表示理论. 创立该理论的最初工作主要是由 G. Frobenius 做的，他的理论建立在复数域上，其主要工具是由他创立的群特征标理论. 与 Frobenius 差不多同时的H. Maschke 与 I. Schur 在群表示的分解与可约性问题上作出了重要贡献. 特别是Schur，经他整理的有限群表示理论简明系统而为较多人所理解，第一个把群与代数的表示理论推广到一般域上的是 E. Noether，她的名著“ Hyperkomplexe Grössen und Darstellungstheorie ”把群与代数的结构理论与表示理论融为一体. 该书对于近世代数的发展产生了深远的影响，在近半个世纪来对群表示理论的各个方面都作出重大贡献的莫过于 R. Brauer，他在诱导特征标与分裂域方面的重要结果已成为群表示理论中最基本的内容

之一．Brauer 的最主要贡献是创立了群的模表示理论，即群在特征数可整除群的阶数的域上的表示理论．

本书将只介绍有限群的常表示理论，我们假定读者已经熟悉线性代数理论，并具备群论、环论与域的伽罗华理论方面的最基本知识，尽管如此，为了便于学习，我们仍在第一章简要地介绍与群表示论有关的群论、域的伽罗华理论与范畴论的基本内容，并比较详尽地讨论有限维代数结构与表示理论，然后从第二章起系统地讨论有限群表示理论．第二、三、四章是关于有限群表示理论的最一般内容，其中包括群表示论的基本概念及研究群表示论两条主要途径的介绍，即有限维代数结构理论和群特征标理论在群表示论上的应用，第五、六、七章着重研究群的诱导表示，其中包括 Mackey 的子群定理与张量积定理，Frobenius 关于限制与诱导表示的互反律，诱导表示的不可约性判则，诱导表示及其特征标的分解以及关于诱导特征标的 Artin 定理与Brauer 定理．最后，第八章专门讨论表示在域上的 Schur 指标．

本书叙述力求简明通俗、自成系统．正文中的例子与每节正文后面的习题可帮助读者理解和拓广正文的内容．

本书可作为高年级大学生与研究生的教科书，也可供有关专业的数学工作者与大学教师阅读．

对于高年级大学生，我们不要求他们预先学过伽罗华理论．同时，以下一些章节的内容可不列入课程范围：§1.2，§1.10，§2.5，§3.2，§4.3，§4.5，§5.5，§6.2 与第八章．此外，§5.1 中关于诱导表示的范畴论刻画的那部分内容也可略去不讲．

目　录

第一章　群表示论的预备知识

在本书里，假定读者已经熟悉关于群论、环论、环上模论、域的伽罗华理论与线性代数理论的基本概念．尽管如此，为了便于讨论群表示理论，也为了使读者了解群表示理论所赖以发展的代数基础，本书仍以一章的篇幅介绍与之有关的知识．

§ 1.1　群论的基本概念

假定读者已熟悉群的基本理论，现在介绍本书中要用到的一些群论基本概念，如不特别申明，本书所考虑的群都是有限群．

(1)　若干特殊群

(1.1.1)　定义　如群 $G\neq 1$ 仅有的正规子群是 G 与 1，则称 G 为**单群**．

如果

$$G=G_1\supseteq G_2\supseteq\cdots\supseteq G_{s+1}=1$$

是群 G 的一个子群序列使 $\forall\, i$，$1\leqslant i\leqslant s$，有 $G_{i+1}\lhd G_i$，这里记号 $G_{i+1}\lhd G_i$ 表明 G_{i+1} 是 G_i 的正规子群，则称该子群列为 G 的长度等于 s 的**正规列**，并称 $\{G_i/G_{i+1}\mid 1\leqslant i\leqslant s\}$ 为该正规列的**因子集**．当因子集由单群组成时，称该正规列为 G 的**合成列**．合成列的因子称为**合成因子**．据 Jordan－Hölder 定理，群 G 的合成列的合成因子集合在同构的意义下与 G 的合成列的选取无关，仅与 G 本身有关，故可称之为 G 的**合成因子集合**．

(1.1.2)　例

(a)　**导群列**　群 G 的导群 $G^{(1)}$ 是 G 的由所有换位子 $\{a^{-1}b^{-1}ab\mid a,b\in G\}$ 所生成的子群，$G^{(1)}$ 也是 G 的使 G/K 为阿贝尔群的最小正规子群 K，定义子群列

$$G=G^{(0)}\supseteq G^{(1)}\supseteq G^{(2)}\supseteq\cdots,$$

这里 $G^{(i)}$ 是 $G^{(i-1)}$ 的导群，$\forall i$，称该子群列为 G 的**导群列**.

(*b*) **下中心列** 定义群 G 的子群列

$$G=G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots,$$

其中 G_i 是由换位子 $\{a^{-1}b^{-1}ab \mid a \in G_{i-1}, b \in G\}$ 生成的子群，$\forall i$，称该子群列为G 的**下中心列**.

(*c*) **上中心列** 定义群 G 的子群列

$$\mathbf{1}=Z_0 \subseteq Z_1 \subseteq Z_2 \subseteq \cdots,$$

其中 Z_1 是 G 的中心. Z_i 是 G 的含 Z_{i-1} 的子群且 Z_i/Z_{i-1} 是 G/Z_{i-1} 的中心，$\forall i$，称该子群列为 G 的**上中心列**.

(1.1.3) 定义 如群 G 的导群列终止于 **1**，则称 G 为**可解群**. 如群 G 的上中心列终止于 G(或等价地，下中心列终止于 **1**)，则称 G 为**幂零群**.

熟知群 G 可解当且仅当 G 有正规子群列

$$G=G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{s+1}=\mathbf{1} \text{(即 } G_i \lhd G,\ \forall i)$$

使 $[G_i : G_{i+1}] := \dfrac{|G_i|}{|G_{i+1}|}$ 是素数幂，$\forall i$，$1 \leqslant i \leqslant s$($|G|$ 表示 G 的阶数).

设 $N \lhd G$. 则 G 可解当且仅当 N 与 G/N 都可解.

(1.1.4) 定义 如群 G 可解，且 G 有合成列

$$G \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{s+1}=1$$

使 $G_i \lhd G$，$\forall i$，则称 G 为**超可解群**.

令 p 为素数，$x \in G$. 如 x 的阶数是 p 的幂，则称 x 为 p **元素**. 如 x 的阶数与 p 互素，则称 x 为 p'**元素**.

显然，恒等元 **1** 既是 p 元素又是 p' 元素. 1 是 G 中仅有的具有这种性质的元素.

$\forall x \in G$，存在唯一分解式 $x=x'x''=x''x'$ 使 x' 为 p' 元素，x'' 为 p 元素，此时称 x' 为 x 的 p'**部分**，x'' 为 x 的 p **部分**.

(1.1.5) 定义 阶数为 p 的幂的群称为 p **群**. 阶数与 p 互素

的群称为 p' **群**.

我们有关于群的集合的如下包含关系:

$\{p$ 群 $|p$ 为素数$\} \subseteq \{$幂零群$\} \subseteq \{$超可解群$\} \subseteq \{$可解群$\}$.

n 个元素组成的集合上的对称群 S_n 与交代群 A_n(A_n 是由 S_n 中所有偶置换组成的子群)当 $n \leqslant 4$ 时是可解群,但当 $n \geqslant 5$ 时不是可解群.

如 G 是幂零群,则 G 的任何真子群 H 的正规化子 K 一定严格包含 H. 群 G 是幂零群的充要条件是 G 为其 Sylow 子群的直积.

还有二族群在表示论中起着重要作用,它们被分别称为初等群与拟初等群.

(1.1.6) 定义 如存在素数 p 使 H 为 p 群 P 与循环 p' 群 Z 的直积:

$$H = P \times Z, \tag{1}$$

则称 H 为 p **初等群**(或简称为**初等群**).

显然,对于任何素数 p,循环群总是 p 初等的;p 群与任何循环群的直积是 p 初等群. 初等群都是幂零群. 初等群的子群也是初等群.

(1.1.7) 定义 如存在素数 p 使 H 为循环 p' 群 Z 与 p 群 P 的半直积:

$$H = Z \rtimes P, \tag{2}$$

则称 H 为 p **拟初等群**(或简称为**拟初等群**).

在拟初等群 H 的分解式(2)中,Z 的取法是唯一的,它是 H 的含有所有 p' 子群的特征子群.

p 拟初等群另有一个等价的定义:如 H 是正规循环子群 A 与 p 群 P 的积:

$$H = AP, \tag{3}$$

则称 H 为 p 拟初等群.

任何初等群都是拟初等的. (2)式中的 p 拟初等群 $H=$

$Z \rtimes P$ 为初等群当且仅当 Z 属于 H 的中心，也当且仅当 H 有正规的 Sylow p 子群.

(Ⅱ) **群在集合上的作用**

(1.1.8) 定义 给定群 G 与集合 Ω. 如 $\varphi:(x,w)\longmapsto xw$ 为从 $G\times\Omega$ 到 Ω 内的映射使 $\forall x,y\in G$ 与 $w\in\Omega$，下式成立：

$$1w=w,$$

$$(xy)w=x(yw),$$

则称 φ 为 G 在 Ω 上的**作用**，称 Ω 为 G **集**. 称两个 G 集 Ω 与 Ω' **为同构的**，记作 $\Omega\cong\Omega'$，如存在双射 $f:\Omega\to\Omega'$ 使

$$f(xw)=xf(w),\quad \forall w\in\Omega,x\in G,$$

这里双射 $f:\Omega\to\Omega'$ 意味着存在映射 $g:\Omega'\to\Omega$ 使 $gf=1_\Omega$ 与 $fg=1_{\Omega'}$，1_Ω 与 $1_{\Omega'}$ 分别为 Ω 与 Ω' 上的恒等映射.

令 Ω 为 G 集. $\forall x\in G$，定义映射 $x_l:\Omega\to\Omega$ 如下：

$$x_lw=xw,\quad \forall w\in\Omega,$$

则有

$$1_l=1_\Omega,(xy)_l=x_ly_l,\quad \forall x,y\in G.$$

故 $x\longmapsto x_l$ 是从 G 到 Ω 上置换群(后者同构于 $|\Omega|$ 次对称群)内的一个同态.

在每个 G 集 Ω 上可定义关系 $\sim$ 如下：令 $v,w\in\Omega$，如存在 $x\in G$ 使 $w=xv$，则记 $v\sim w$. 这是一个等价关系. 相应的等价类称为 G **轨道**，或简称为**轨道**. 每个轨道也都是 G 集. 由一个轨道组成的 G 集称为**可迁** G **集**.

(1.1.9) 定义 令 Ω 为 G 集，$w\in\Omega$. 定义 w 在 G 中的**稳定子**为

$$\mathrm{Stab}_G(w):=\{x\in G\mid xw=w\}.$$

注意 $\mathrm{Stab}_G(w)$ 是 G 的子群. 如 H 是 G 的子群，则左陪集空间 $G/H=\{yH\mid y\in G\}$ 在 G 的如下作用下形成可迁 G 集：

$$(x,yH)\longmapsto xyH,\quad \forall x,y\in G.$$

此时，$H=\mathrm{Stab}_G(H)$.

以下命题刻画了有限 G 集.

(1.1.10) 命题 令 Ω 为 G 集.

(a) 设 Ω 是可迁的，$w, w' \in \Omega$，$H = \mathrm{Stab}_G(w)$ 与 $H' = \mathrm{Stab}_G(w')$. 则存在某 $x \in G$ 使 $w' = xw$，且 $H' = xHx^{-1}$. 特别存在 G 集同构 $\Omega \cong G/H \cong G/H'$.

(b) 设 Ω 是可迁的. 设 G 与 Ω 作为集合都是有限的. 则

$$|\Omega| = [G : \mathrm{Stab}_G(w)], \quad \forall w \in \Omega.$$

特别，$|\Omega| \mid |G|$.

(c) 设 Ω 是有限集(不必可迁). 令 $\{\Omega_i \mid i \in I\}$ 为 Ω 的 G 轨道集合，则有

$$|\Omega| = \sum_{i \in I} |\Omega_i|$$

与 $|\Omega_i| = [G : \mathrm{Stab}_G(w_i)]$，$\forall w_i \in \Omega_i$，$i \in I$.

(1.1.11) 例

(a) 设 H 是 G 的子群，则 H 可通过左乘 $(h, x) \longmapsto hx$ 作用于 G，也可通过右乘 $(x, h) \longmapsto xh^{-1}$ 作用于 G，这里 $x \in G$，$h \in H$. 在第一种情形的 H 轨道是右陪集 $\{Hx\}$，而在第二种情形的 H 轨道是左陪集 $\{xH\}$.

(b) 设 H, K 是 G 的二个子群. 则直积 $H \times K$ 以如下方式作用于 G:

$$((h, k), x) \longmapsto hxk^{-1}, \quad \forall x \in G, h \in H, k \in K.$$

此时的轨道是 (H, K)双陪集 $\{HxK\}$.

(c) 设 H 是 G 的子群. H 可通过 G 的内自同构作用于 G:

$$(x, y) \longmapsto xyx^{-1} = i_x(y), \quad \forall x \in H, y \in G,$$

这里 i_x 是 G 的由 x 所决定的内自同构. 同态 $x \longmapsto i_x$ 把 H 映到 G 的内自同构群内. 其核恰为 H 与 G 的中心 $Z(G)$的交集 $H \cap Z(G)$. 此时的 H 轨道称为 G 的 H **共轭类**. 特别，

当 $H=G$ 时，H 轨道正好是 G 的共轭类．如 $\mathscr{C}$ 是 G 的共轭类，$x\in\mathscr{C}$，则 x 在 G 中的稳定子是 x 在 G 中的中心化子

$$C_G(x):=\{y\in G\mid yxy^{-1}=x\}.$$

我们有 G 的类方程

$$|G|=|Z(G)|+\sum_x [G:C_G(x)],$$

右端和式里的 x 取遍 G 在 $G-Z(G)$ 中共轭类的一个代表系．

(Ⅲ) 群由生成元与关系式来定义

(1.1.12) 定义 设 G 是群．$a_1,\cdots,a_n\in G$．$\{w_1,\cdots,w_t\}$ 是元素 $a_i(1\leqslant i\leqslant n)$ 及其逆元的一些乘积．它们满足条件：

(*a*) $G=\langle a_1,\cdots,a_n\rangle$(即 G 是由元素 $a_1,\cdots,a_n$ 生成的)，且关系式 $w_1=1,\cdots,w_t=1$ 都成立．

(*b*) 如 G' 是含元素 $a_1',\cdots,a_n'$ 的另外一个群使得 $w_1'=\cdots=w_t'=1$ 在 G' 中成立，这里 $\forall i$，$1\leqslant i\leqslant t$，w_i' 可从 w_i 通过把因子 $a_j(1\leqslant j\leqslant n)$ 换成 a_j' 而得，则存在群的唯一同态 $\varphi:G\to G'$ 使 $\varphi(a_i)=a_i'$，$\forall i$，$1\leqslant i\leqslant n$，并称 G 有一个**表现**

$$G=\langle a_1,\cdots,a_n\mid w_1=w_2=\cdots=w_t=1\rangle.$$

由定义可知：有相同表现的二个群是同构的．

(1.1.13) 例

(*a*) 阶数为 $2n$ 的二面体群 D_n 有表现

$$D_n=\langle r,s\mid r^n=s^2=(rs)^2=1\rangle.$$

(*b*) 阶数为 $4m$ 的广义四元数群 Q_m 有表现

$$Q_m=\langle r,s\mid r^{2m}=r^ms^2=rsrs^{-1}=1\rangle.$$

(*c*) 有限生成的 Coxeter 群 W 有表现

$$W=\langle s_1,\cdots,s_n\mid (s_is_j)^{m_{ij}}=1,\ \forall i,j,1\leqslant i,j\leqslant n\rangle,$$

这里正整数 m_{ij} 满足

$$m_{ij}=m_{ji}\begin{cases}=1, & \text{如 } i=j,\\ >1, & \text{如 } i\neq j.\end{cases}$$

注意对称群 S_n 是 Coxeter 群，它有表现

$$S_n=\langle s_1,\cdots,s_{n-1}\mid (s_is_j)^{m_{ij}}=\mathbf{1},\ \forall i,j,1\leqslant i,j<n\rangle,$$

这里

$$m_{ij}=\begin{cases}1,\text{如 } i=j,\\ 2,\text{如 } i\neq j\pm 1,j,\\ 3,\text{如 } i=j\pm 1.\end{cases}$$

习　题

1．设 $H=C\times P$ 是 p 初等群，这里 C 是循环 p' 群，P 是 p 群．求证：

(a)　H 是幂零群．H 的每个子群都是 p 初等群．

(b)　C 是 H 中所有 p' 元素的集合．P 是 H 中所有 p 元素的集合．

2．验证拟初等群的子群也是拟初等群．

3．设 X 是 G 集．如 $\forall (u,v),(u',v')\in X\times X,u\neq v,u'\neq v'$，存在 $g\in G$ 使 $gu=u'$ 与 $gv=v'$，则称 X 为**双可迁的**．设 G 是集合 $X=\{x_1,\cdots,x_n\}$ 上可迁置换群(即 G 是满足以下条件的群：$\forall 1\leqslant i,j\leqslant n$，存在 $g\in G$ 使 $gx_i=x_j$)．令 $H=\{g\in G\mid gx_1=x_1\}$．求证：

(a)　存在元素 $g_1,\cdots,g_n\in G$ 使 $g_i(x_1)=x_i,1\leqslant i\leqslant n$，且

$$G=g_1H\cup\cdots\cup g_nH.$$

(b)　X 上 H 轨道的个数等于 G 的 (H,H) 双陪集个数．

(c)　如 G 双可迁地作用于 X，则 H 可迁地作用于 $X-\{x_1\}$．

4．设 H,H' 与 K 是 G 的子群．如存在 $k\in K$ 使 $H'=kHk^{-1}$，则称 H 与 H' 为 K **共轭的**．验证 G 的 K 共轭于 H 的相异子群个数等于 $[K:N_K(H)]$，这里 $N_K(H):=\{k\in K\mid H=kHk^{-1}\}$．

5．试证存在严格的包含关系：

$$\{\text{幂零群}\}\subset\{\text{超可解群}\}\subset\{\text{可解群}\}.$$

§ 1.2　伽罗华理论

本节概要地叙述后面要用到的伽罗华理论中一些定义和结果．

如 F 是域 E 的子域，则称 E 为 F 的**扩域**，记作 E/F．

此时 E 可自然地看作 F 空间，其维数记作 $\dim_F E$. 如 $\dim_F E < \infty$，则称 E/F 为**有限扩域**. 如 $\dim_F E = \infty$，则称 E/F 为**无限扩域**.

如域 K 满足 $E \supset K \supset F$，则称 K 为 E/F 的**中间域**. 此时如 E/F 是有限扩域，则等式 $\dim_F E = \dim_K E \cdot \dim_F K$ 成立.

记 $F[x]$ 为关于不定元 x 的系数属于域 F 的多项式组成的环. 设 $u \in E/F$. 如存在某非零多项式 $f \in F[x]$ 使得 $f(u)=0$，则称 u 为 F **上代数元**. 此时，在 $F[x]$ 中存在唯一的满足等式 $g(u)=0$ 的次数最小的首一项式 $g(x)$（最高次项系数等于 1 的多项式称为**首一多项式**），称 $g(x)$ 为 u 在 F **上的最小多项式**. $g(x)$ 的次数称为 u **的次数**，由 F 上代数元组成的扩域称为**代数扩域**. 由 F 上所有代数元组成的扩域称为 F **上的代数闭域**，或简称**代数闭域**. 由定义知，$F[x]$ 中任一正次数多项式在 F 上的代数闭域内有根.

如 S 是扩域 E/F 的子集，则由 $F \cup S$ 在 E 内生成的子域称为 S 在 F 上生成的子域，记作 $F(S)$，由 $F \cup S$ 在 E 内生成的子环称为 S 在 F 上生成的子环，记作 $F[S]$. 显然，$F[S]$ 必是整环，特别，当 S 是 F 上代数元集合时，我们有 $F(S)=F[S]$.

设 E/F 是 F 的扩域，$f \in F[x]$. 如 f 在 $E[x]$ 内可分解为一次因子的乘积，则称 f 在 E/F 上**分裂**. 显然，f 在 E 上分裂当且仅当 E 包含 f 的全部根. 使 f 在其上能分裂的最小扩域 E/F 称为 f 在 F 上的**分裂域**，熟知 f 在 F 上的分裂域是有限扩域.

设 E/F 是代数扩域. 如果 $F[x]$ 内任何不可约多项式只要在 E 内有一个根，它就在 $E[x]$ 内分裂成一次因子的乘积，则称 E/F 为**正规扩域**. 特别，F 上的代数闭域是正规扩域.

我们知道，有限扩域 E/F 是正规扩域当且仅当 E/F 是某一多项式 $f \in F[x]$ 的分裂域.

设$f\in F[x]$. 如果f 在$F[x]$ 内的每个不可约因子都只有单根，则称f在F 上**可离**. 设u 是F 上代数元. 如u 在F 上的最小多项式是可离多项式，则称u 为F 上**可离元**. 如果代数扩域E/F 的每个元素都是F 上可离元，则称E/F 为**可离扩域**. 记域F 的特征数为char. F. 则当char. $F=0$ 时，E/F 总是可离扩域.

给定二个扩域E/F 与E'/F. 如果$\sigma: E\to E'$是域同态(或域同构)使得$\sigma(x)=x$，$\forall x\in F$，则称σ 为F **同态**(或F **同构**)，令$u\in E$ 与$u'\in E'$为F 上代数元，则要使u 与u'是同一不可约多项式$f\in F[x]$ 的根当且仅当存在F 同构$\sigma: F(u)\to F(u')$使得$\sigma(u)=u'$.

特别，取$E'=E$，此时称σ 为E 的F **自同构**. E 的F 自同构全体形成一个群，记作 Gal E/F，称为E **在**F **上的伽罗华群**. 当E/F 是有限扩域时，我们有$|\text{Gal } E/F|\leqslant \dim_F E$. 等号成立当且仅当$E/F$ 是正规可离扩域.

设$f\in F[x]$，E/F 是f 在F 上的分裂域. 则E/F 在F 同构的意义下由f 所唯一确定，称Gal E/F 为f **在**F**上的伽罗华群**.

给定$u, u'\in E/F$. 如存在$\sigma\in\text{Gal } E/F$ 使得$u'=\sigma(u)$，则称u 与u'在F 上**伽罗华共轭**. 这是E/F 中的一个等价关系，相应的等价类称为F 上的**伽罗华共轭类**. $u\in E/F$ 所在的F 上伽罗华共轭类的基数 $\leqslant \dim_F F(u)$. 等号成立当且仅当E/F 是正规扩域且u 是F 上可离元.

设E/F 是正规扩域，K, K'是E/F 的中间域. 如存在$\sigma\in\text{Gal } E/F$ 使得$K'=\sigma(K)$，则称K 与K'在F 上**共轭**.

设E/F 是正规扩域，K 是E/F 的中间域. 如存在F 同态$\tau: K\to E$，则τ 必可扩充为E 的F 自同构.

设E/F 是扩域、如果存在Gal E/F 的一个子群G 使得

$$F=\text{Inv}_G(E):=\{x\in E\mid \sigma(x)=x,\ \forall\sigma\in G\},$$

则称 E 为 F 的**伽罗华扩域**，或称 E/F 为**伽罗华**的.

熟知 E/F 是有限伽罗华扩域当且仅当 E/F 是有限次正规可离扩域.

设 E/F 是有限伽罗华扩域，$G=\mathrm{Gal}\ E/F$. 对于 E/F 的任何中间域 K，可以定义 G 的一个子群

$$\mathrm{Gal}\ E/K=\{\sigma\in G\mid \sigma(x)=x,\quad \forall x\in K\}.$$

对于 G 的任何子群 H，可以定义 E/F 的一个中间域

$$\mathrm{Inv}_H(E)=\{x\in E\mid \sigma(x)=x,\quad \forall\sigma\in H\}.$$

则 $K\longmapsto \mathrm{Gal}\ E/K$，$H\longmapsto \mathrm{Inv}_H(E)$ 在 G 的所有子群与 E/F 的所有中间域之间定义了一个逆序双射. 设 H_1，H_2 分别是 G 的与中间域 K_1，K_2 相对应的子群，则 K_1，K_2 在自同构 $\sigma\in G$ 之下共轭当且仅当 H_1 与 H_2 是 G 的共轭子群：$H_2=\sigma H_1\sigma^{-1}$. 特别，$K/F$ 是正规扩域当且仅当 $\mathrm{Gal}\ E/K=H$ 是 G 的正规子群. 此时，$\mathrm{Gal}\ K/F\cong G/H$.

下面我们要考虑一个特殊的伽罗华扩域.

方程 $x^n=1$ 的根称为 n 次单位根，在任何域 F 内，$x^n=1$ 的根全体关于乘法形成一个循环群. 如 $\xi\in F$ 满足

$$\xi^k=1\Longleftrightarrow n\mid k\ (\text{记号 } n\mid k \text{ 表示 } n \text{ 整除 } k),$$

则称 ξ 为 n **次单位原根**. 对于正整数 n，令 $\varphi(n)$ 为集合 $\{1,2,\cdots,n\}$ 中与 n 互素的整数个数，称 $\varphi(n)$ 为**欧拉函数**. 熟知 $\varphi(n)$ 恰等于 n 次单位原根的个数. 欧拉函数满足如下性质：

(a) 如 $(m,n)=1$，则 $\varphi(mn)=\varphi(m)\varphi(n)$.

(b) 如 p 是素数，$e>0$，则 $\varphi(p^e)=p^{e-1}(p-1)$.

设 $\xi_1,\cdots,\xi_r$ 是所有 n 次单位原根，这里 $r=\varphi(n)$，则多项式

$$\Phi_n(x)=\prod_i(x-\xi_i)$$

称为 n **次分圆多项式**，它的次数是 $\varphi(n)$. 熟知有理数域 $\mathbb{Q}$ 上的分圆多项式是不可约的.