若尔当-赫尔德定理

2024 年 12 月 27 日

目录

1 若尔当-赫尔德定理 . . . 2

1.1 引理：扎森豪斯引理 . . . 2
1.2 定义：合成列 . . . 3
1.3 命题： . . . 3
1.4 定义：等价 . . . 4
1.5 定义：加细 . . . 4
1.6 定理：施赖埃尔加细定理 . . . 4
1.7 定理：若尔当-赫尔德定理 . . . 5
1.7.1 例子 . . . 6
1.8 定义：扩张 . . . 6
1.8.1 例子 . . . 6
1.9 命题： . . . 7
1.10 定义：换位子 . . . 8
1.11 命题 . . . 8
1.11.1 例子 . . . 9
1.12 定义：导出列 . . . 9
1.13 命题 . . . 9
1.14 定义：降中心列 . . . 10

1 若尔当-赫尔德定理

迦罗瓦引进群研究$k[x]$中的多项式，其中k是特征为0的域，并且发现这样的多项式是可解的当且仅当他的迦罗瓦群是可解群。这章节就详细的研究可解群。

回想群G的合成列是有限群序列，$G = G_0, G_1, \cdots, G_n = \{1\}$使得：

$$G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_n = \{1\}$$

且$G_{i+1} \lhd G_i$对所有i成立。这个序列的因子群是群$G_0/G_1, G_1/G_2, \cdots, G_{n-1}/G_n$，序列的长度是其非平凡因子群的个数，我们说$G$是可解的，若在其合成列中，因子群都是素数阶循环群。

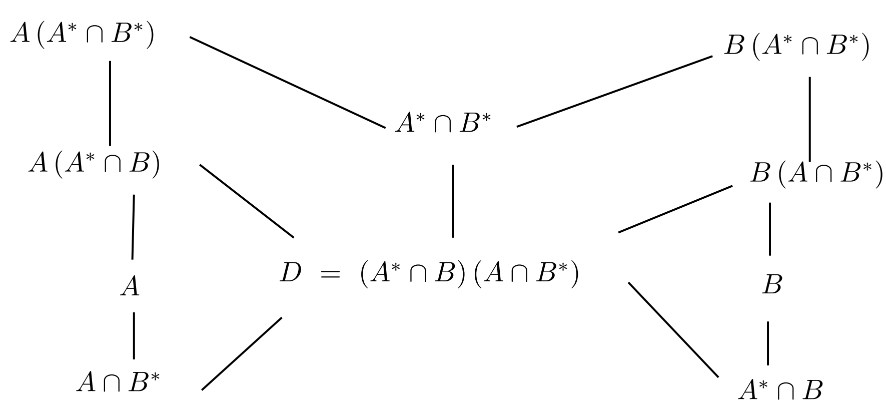
我们要比较一个群的不同的正规列，先从推广一个第二同构定理的一个技巧性结果开始：

1.1 引理：扎森豪斯引理

给定群G的四个子群$A \lhd A^*, B \lhd B^*$，则$A(A^* \cap B) \lhd A(A^* \cap B^*)$，$B(B^* \cap A) \lhd B(B^* \cap A^*)$，则这里有一个同构

$$\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \cong \frac{B(B^* \cap A^*)}{B(B^* \cap A)}$$

注： 扎森豪斯定理也被称为蝴蝶引理，因为他可以表示为下图的形式：



该同构是对称的，因为可以通过交换符号A和B从左侧推出右侧

证明： 我们断言$(A\cap B^*)\lhd(A^*\cap B^*)$，即若$c\in A\cap B^*$和$x\in A^*\cap B^*$，则$xcx^{-1}\in A\cap B^*$(注意$A\cap B^*$是正规子群)。现在，由于$A\lhd A^*$，则$c\in A,x\in A^*$有$xcx^{-1}\in A$，而且，由于$c,x\in B^*$同样的我们也可以得到$xcx^{-1}\in B^*$。由于正规子群的正规子群依然是正规子群，很容易得到$(A\cap B^*)\lhd(A^*\cap B^*)$。类似的讨论可以得到$(A^*\cap B)\lhd(A^*\cap B^*)$。

因此，由$D=(A\cap B^*)(A^*\cap B)$定义的子集D是$A^*\cap B^*$的一个正规子群[1]。

利用注释中的对称性，我们来证明下述同构：

$$\frac{A(A^*\cap B^*)}{A(A^*\cap B)}\to\frac{A^*\cap B^*}{D}$$

定义$\varphi:A(A^*\cap B^*)$为$\varphi:ax\to xD$，其中$x\in A$而$x\in A^*\cap B^*$。可以验证φ是well-defined的。若$ax=a'x'$，其中$a'\in A,x'\in A^*\cap B^*$，则$(a')^{-1}a=x'x^{-1}\in A\cap(A^*\cap B^*)=A\cap B^*\leq D$。同样，$\varphi$也是同态，$axa'x'=a''xx'$，其中$a''=a(xa'x^{-1})\in A$，那么$\varphi(axa'x')=\varphi(a''xx')=xx'D=\varphi(ax)\varphi(a'x')$。$\varphi$是一个满射，且$\ker\varphi=A(A^*\cap B)$利用第一同构定理即可证明完毕。最后，我们可以用对称性推出命题一开始关于B的部分。

1.2 定义：合成列

合成列指的是非平凡因子群都是单群的正规列，合成列的非平凡因子群叫做G的合成因子。

群不一定有合成列，例如阿贝尔群$\mathbb{Z}$就没有，但每个有限群都存在合成列。

1.3 命题：

每个有限群都有合成列

证明： 若命题为假，令G是满足没有合成列的阶是最小的有限群，由于G不是单群，否则$G>\{1\}$是合成列，因此G有正规真子群H，我们假设H是极

[1] 正规子群乘子群得到的仍然是子群。特别的两个正规群乘积依然是正规群

大正规子群，从而G/H是单群[2]

。且$|H| < |G|$，所以H有合成列，例如$H = H_0 > H_1 > \cdots > \{1\}$，但$G > H_0 > \cdots > \{1\}$就是$G$的合成列，矛盾

群G是可解的，若他有正规列并且正规列的因子群都是素数阶循环群。而素数阶循环群都是单群，所以可解群中的正规列是合成列，从而可知G的合成因子是素数阶循环群。

1.4 定义：等价

群G的两个正规列称为等价的，若对每个正规列的非平凡因子群的集合之间存在双射使得对应的因子群同构。

1.5 定义：加细

一个正规列的加细是吧原始的正规列作为子序列的正规列$G = N_0, N_1, \cdots, N_k = \{1\}$

换句话说，一个正规列的加细指的是在原来的正规列中添加更多的子群形成一个新的正规列。

注意一个合成列只允许无关紧要的加细，也就是只能插入重复的项。注意G_i/G_{i+1}是单群的话，那么理应上是不存在任何的中间子群L使得$G_i > L > G_{i+1}$且$L \lhd G_i$。因为单群不存在任何的真正规子群。所以任一合成列的加细都等价于它本身原始的合成列。

1.6 定理：施赖埃尔加细定理

群G的任意两个正规列

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

和

$$G = N_0 \geq N_1 \geq \cdots \geq N_k = \{1\}$$

有等价的加细。

[2]简单的证明一下：N是G的极大正规子群当且仅当G/N是单群，证明：定义映射$f: G \to G/N$，若G/N是单群，则N是G的极大正规子群。不妨假设H是真包含N的G的正规子群，由第三同构定理，有$G/H \cong (G/N)(H/N)$，接着使用对应定理，H包含N就有H/N是G/N的正规真子群，与G/N是单群矛盾。反过来，G/N是单群，则G/N不存在中间群，由对应定理，N是极大正规子群。

证明： 注意，这是一个构造性的证明。对每个$i \geq 0$定义

$$G_{ij} = G_{i+1}(G_i \cap N_j)$$

现在，$N_0 = G$，那么有

$$G_{i0} = G_{i+1}(G_i \cap G) = G_{i+1}G_i = G_i$$

其次，$N_k = \{1\}$，所以

$$G_{ik} = G_{i+1}(G_i \cap N_k) = G_{i+1}$$

那么我们就得到了，G_{ij}是G_i的列的子序列:

$$\cdots \geq G_i = G_{i0} \geq_{i1} \geq \cdots \geq G_{ik} = G_{i+1} \geq \cdots$$

另一方面，对子群N_{pq}，有

$$N_{pq} = N_{p+1}(N_p \cap G_q)$$

得到第二个列的子序列。我们就把两个列都拓展到nk个项，现在，对每对i, j和四个子群$G_{i+1} \lhd G_i$以及$N_{j+1} \lhd N_j$，蝴蝶引理表明两个子序列都是正规列，所以这是一个加细，且存在同构

$$\frac{G_{i+1}(G_i \cap N_j)}{G_{i+1}(G_i \cap N_{j+1})} \cong \frac{N_{j+1}(N_j \cap G_i)}{N_{j+1}(N_j \cap G_{i+1})}$$

也就是

$$G_{i,j}/G_{i,j+1} \cong N_{j,i}/N_{j,i+1}$$

结合这是个同构映射，表明了两个加细是等价的。

1.7 定理：若尔当-赫尔德定理

一个群G的任意两个合成列等价，特别地，如果合成列存在，则合成列的长度是G的不变量。

证明： 合成列的任意加细都等价于原来的合成列，利用施赖埃尔定理可知任意两个合成列等价。

1.7.1 例子

设$G = \mathrm{GL}(2, F_4)$是元素在F_4是元素在只有4个元素的域中的一切2×2非奇异矩阵的一般线性群。

现在，$\det : G \to (F_4)^\times$，其中$(F_4)^\times \cong I_3$是$F_4$的非零元素乘法群，现在，$\ker\det = \mathrm{SL}(2, F_4)$，即那些行列式为1的矩阵组成的特殊线性群。那么就存在正规列

$$G = \mathrm{GL}(2, F_4) \geq \mathrm{SL}(2, F_4) \geq \{1\}$$

注意$\mathrm{SL}(2, F_4) \cong A_5$，但我们还不能说$G$是不可解的，因为可解性的定义要求具有素数因子群的合成列，但未必是这一个。然而若尔当-赫尔德定理告诉我们，G的合成列其因子都应该是素数阶，并且长度一致。从而可以知道$\mathrm{GL}(2, F_4)$是不可解的。

1.8 定义：扩张

若G是群且$K \lhd G$，则G称为K和G/K的扩张

1.8.1 例子

给定正规子群K和他的商群$Q = G/K$，则直积$K \times Q$也是Q和K的扩张。

对一给定的群K和Q，K, Q的扩张恒存在（直积），但可能有不同构于这种扩张的扩张。一般说，若我们把K和Q的扩张看做是K和Q的一个乘积，则这个乘积不是唯一的。扩张问题是对于给定的一对群K, Q的一切可能的扩张进行分类

假设G有正规列

$$G = K_0 \geq K_1 \geq K_2 \geq \cdots \geq K_{n-1} \geq K_n = \{1\}$$

其因子群记为$Q_1, \cdots, Q_n$，对一切$i \geq 1$有

$$Q_i = K_{i-1}/K_i$$

现在，$K_n = \{1\}$，则$Q_n = K_{n-1}$。最重要的是，$K_{n-2}/K_{n-1} = Q_{n-1}$，从而$K_{n-2}$是$K_{n-1}$和$Q_{n-1}$的扩张，若我们能解决扩张问题，则可以从$K_{n-1}$和$Q_{n-1}$，也就是从$Q_n$和$Q_{n-1}$得到$K_{n-2}$，下一步我们考虑$K_{n-3}/K_{n-2} = Q_{n-2}$，从而$K_{n-3}$是$K_{n-2}$和$Q_{n-2}$的扩张，如果我们能解决扩张问题，则可以从$K_{n-2}$和$Q_{n-2}$取

回K_{n-3}。以此类推，沿着合成列往上最终$G = K_0$可以从合成列$Q_n, Q_{n-1}, \cdots, Q_1$取回。所以$G$就是因子群的乘积。若正规列是合成列，则若尔当-赫尔德定理说这个乘积的因子是被G唯一确定的。所以，只要了解有限单群且能解决扩张问题，我们就可以知道有限群的真面目。

我们现在跳过一般群的叙述，转而考察可解群，可解群是为确定运用根式可解的多项式而产生的，然而有不直接涉及伽罗瓦理论和关于可解群的纯群论理论，霍尔的一个推广西罗定理如下：若G是阶为ab的可解群，其中a, b互素，则G有一个a阶子群，此外，任意的两个这样的子群共轭，而伯恩赛德引理说，$| G |= p^m q^n$，其中p, q是素数，则G是可解群。而费特汤普森定理说，每个奇数阶群必是可解群。

1.9 命题：

有限$p-$群都是可解群

证明： 若G是阿贝尔群，则G一定是可解群。[3]，否则若G不是阿贝尔群，则它的中心$Z(G)$是非平凡真正规阿贝尔子群，由于$Z(G)$是阿贝尔群，所以它是可解群。现在，$Z(G)$本身也是素数阶群，用归纳法，$| Z(G) | || G |$可知存在一合成列，使得$G/Z(G)$是素数阶，因此它可解。另外，由于$Z(G)$可解，且$G/Z(G)$可解，由下述定理可知G是可解的：

若$H \lhd G$且G/H是可解群，则G是可解群

证明： 由于G/H可解，则存在正规列

$$G/H \geq K_1^* \geq \cdots \geq K_m^* = \{1\}$$

是素数阶因子群，又对应定理，则存在关于G的子群K_i有

$$G \geq K_1 \geq K_2 \geq \cdots \geq K_m = H$$

其中对一切$i, K_i/H = K_i^*$且$K_{i+1} \lhd K_i$，由第三同构定理，$K_i^*/K_{i+1}^* \cong K_i/K_{i+1}$，所以对一切$i, K_i/K_{i+1}$是素数阶循环群。现在，$H$是可解的，存在正规列

$$H \geq H_1 \geq H_2 \geq \cdots \geq H_q = \{1\}$$

[3]阿贝尔群是单群当且仅当p是素数。证明：素数阶阿贝尔群合成列是平凡的，只有G和{1}

只需要把两者连接起来就得到了关于G的合成列了。

因此G是可解群

1.10 定义：换位子

若G是群且$x, y \in G$，则它们的换位子$[x, y]$指的是元素

$$[x, y] = xyx^{-1}y^{-1}$$

若X和Y是G的子群，则$[X, Y]$定义为

$$[X, Y] =< [x, y] : x \in X, y \in Y >$$

特别的G的换位子群G'指的是

$$G' = [G, G]$$

即由一切换位子生成的子群

从定义可以推出，若群的两个元素可以交换，则$[x, y] = 1$。

1.11 命题

设G是群

1. 换位子群G'是G的正规子群，且G/G'是阿贝尔群
2. 若$H \lhd G$且G/H是阿贝尔群，则$G' \leq H$

证明： 换位子的$xyx^{-1}y^{-1}$的逆本身也是换位子，注意$[x, y]^{-1} = yxy^{-1}x^{-1} = [y, x]$，所以$G'$对换位子是封闭的，每个元素都是换位子的积。而换位子的共轭也是换位子，注意

$$\begin{aligned} a[x, y]a^{-1} =& a(xyx^{-1}y^{-1})a^{-1} \\ =& axa^{-1}aya^{-1}ax^{-1}a^{-1}ay^{-1}a^{-1} \\ =& [axa^{-1}, aya^{-1}] \end{aligned}$$

因此$G' \lhd G$。

若$aG', bG' \in G/G'$，则验证阿贝尔群的5条性质

$$aG'bG'(aG')^{-1}(bG')^{-1} = aba^{-1}b^{-1} = [a,b]G' = G'$$

所以G/G'是阿贝尔群

证明2： 设$H \lhd G$且G/H是阿贝尔群，若$a, b \in G$，则$aHbH = bHaH$，即$abH = baH$，从而$b^{-1}a^{-1}ba \in H$，每个换位子都形如$b^{-1}a^{-1}ba$，就有$G' \leq H$

1.11.1 例子

1. 从定义可以推导出G是阿贝尔群当且仅当$G' = \{1\}$
2. 若G是单群，由于G'是正规群，因此$G' = \{1\}$或者$G' = G$。当G的阶是素数出现第一种情况，否则出现第二种。特别的，对$n \geq 5$，$(A_n)' = A_n$

1.12 定义：导出列

G的导出列指的是

$$G = G^{(0)} \geq G^{(1)} \geq \cdots \geq G^{(i)} \geq G^{(i+1)} \geq \cdots$$

其中$G^{(0)} = G, G^{(1)} = G'$，更一般的，对所有$i \geq 0$，$G^{(i+1)} = (G^{(i)})' = [G^{(i)}, G^{(i)}]$

可以验证，$G^{(i)}$是全不变子群，因此$G^{(i)} \lhd G$。意味着$G^{(i+1)} \lhd G^{(i)}$，所以导出列是正规列。当G是可解的时候意味着导出列到达$\{1\}$

1.13 命题

1. 有限群G是可解群当且仅当有正规列，且因子群是阿贝尔群
2. 有限群G是可解群当且仅当存在某个n使得

$$G^{(n)} = \{1\}$$

证明： G是可解群，则G存在正规列，其因子群G_i/G_{i+1}是素数阶循环群，因此是阿贝尔群。

反过来，若G有因子群都是阿贝尔群的正规列，则任意加细因子群也是阿贝尔群，特别的G是有限群，那就有G的合成列，这个合成列的因子群都是阿贝尔单群，因此都是素数阶循环群，有G是可解的

证明2： 我们假定G是可解的，那么就有正规列

$$G \geq G_1 \geq \cdots \geq G_n = \{!\}$$

它的因子群G_i/G_{i+1}是阿贝尔群。现在，我们对$i \geq 0$进行归纳，证明$G^i \leq G_i$，首先，$G^{(0)} = G = G_0$是成立的，对于归纳步骤，由于G_i/G_{i+1}是阿贝尔群，利用命题1.11的2.就有$(G_i)' \leq G_{i+1}$，接着，归纳假设对$G^{(i)} \leq G_i$是成立的，就有

$$G^{(i+1)} = (G^{(i)})' \leq (G_i)' \leq G_{i+1}$$

特别的，$G^{(n)} \leq G_n = \{1\}$，这就是我们想要的。

反过来，设$G^{(n)} = 1$，则导出列是正规列，其次，$G^{(n)} = 1$当且仅当$G^{(n)}$是阿贝尔群，那么他有一个阿贝尔因子群，利用命题1，G是可解的。

一个简单的例子是，令$G = S_4$，它的导出列为

$$S_4 > A_4 > V > \{(1)\}$$

早先定义的可解群只适用于平凡群，但命题给出的是针对一切群，甚至可以是无限群。我们把一个群的导出列经过有限步达到$\{1\}$作为可解群的新定义，根据这个新定义，每个阿贝尔群都是可解群。但原来的定义说，阿贝尔群是可解当且仅当它们都是有限的。

此外，用正规列还可以定义其他重要的群类其中重要一个是由幂零群组成的：

1.14 定义：降中心列

群G的降中心列指的是：

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots$$

其中$\gamma_{i+1}(G) = [\gamma_i(G), G]$，群$G$称为幂零群，若降中心列达到$\{1\}$，即对某个$n$有$\gamma_n(G) = \{1\}$

注意$\gamma_2(G) = G'$，但随后导出列和降中心列可能是不同的，例如$\gamma_3(G) = [G', G] \geq G^{(2)}$，且很可能是严格的不等式