

伽罗瓦理论的基本思想就是用群论的思想方法，
分析和解方程的根式求解问题
因此，在这节简单讨论一些与有限可解群有关的结果，

定义 7.1 设 G 是群， a, b 属于 G ，称 $aba^{-1}b^{-1}$ 是 a, b 的换位子
群 G 中由所有换位子生成的子群，称为 G 的换位子群，记为 $[G, G]$

命题 7.1 设 G 是群，则

- (1) $[G, G]$ 是群 G 的正规子群，
- (2) 若 H 是 G 的正规子群，则当且仅当 H 包含 $[G, G]$ 时， G/H 是交换群
- (3) $G/[G, G]$ 是交换群，

证: (1) 对属于 G 的任意 a, b, g ,

只需考察 $g(aba^{-1}b^{-1})g^{-1} = gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1}$

$= (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1}$ 属于 $[G, G]$,

(2) 当且仅当对属于 G 的任意 a, b , G/H 是交换群时，有 $aHbH = bHaH$

而这又等价于 $abH = baH$, $a^{-1}b^{-1}ab$ 属于 H ,

而最后一个关系式成立的充要条件恰为 H 包含 $[G, G]$,

(3) 由(1)和(2)立即可得

一般地，用 $G^{(1)}$ 表示换位子群 $[G, G]$ ，即 $G^{(1)} = [G, G]$ ，

并且定义 $G^{(0)} = G$, $G^{(k)} = (G^{(k-1)})^{(1)} = [G^{(k-1)}, G^{(k-1)}]$, $k = 2, 3, \dots$,

这样我们就得到一个下降的子群列 $G \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \dots \supseteq G^{(k-1)} \supseteq G^{(k)} \supseteq \dots$,

其中每一项 $G^{(k)}$ 都是其前一项 $G^{(k-1)}$ 的正规子群，且 $G^{(k-1)}/G^{(k)}$ 是交换群，

定义 7.2 令 G 是一个群，若存在正整数 n ，使得 $G^{(n)} = \{1\}$ ，则称 G 是可解群

显然，所有的交换群都是可解群，

例 7.1 试证明对称群 S_3, S_4 是可解群，

解: 由换位子群的定义可知 $[S_n, S_n]$ 包含于 A_n

又根据任意偶置换可以写成长度为 3 的轮换的乘积，

以及 $(acb) = (abc)(ab)(abc)^{-1}(ab)^{-1}$ ，可推得 A_n 包含于 $[S_n, S_n]$ ，

因此， $[S_n, S_n] = A_n$

因为 $A_3 = \{(1), (123), (132)\}$ ，

所以为求 $(A_3)^{(1)}$ ，仅需计算 $(123)(132)(123)^{-1}(132)^{-1}$ 即可，

计算得 $(A_3)^{(1)} = \{(1)\}$ ，即 $(S_3)^{(2)} = \{(1)\}$ ，所以 S_3 是可解群，

计算可知 $(A_4)^{(1)} = \{(1), (12)(34), (13)(24), (14)(23)\}$ ， $(S_4)^{(3)} = (A_4)^{(2)} = \{(1)\}$ ，

因此， S_4 是可解群

例 7.2 证明非交换单群不是可解群，

证: 设 G 是非交换单群，

因为 $G^{(1)}$ 是单群 G 的正规子群，所以， $G^{(1)} = \{1\}$ 或 $G^{(1)} = G$ ，

因为 G 不是交换群，所以只能有 $G^{(1)} = G$ ，

那么对任意正整数 n ， $G^{(n)} = G \neq \{1\}$ ，因此， G 不是可解群，

命题 7.2(1)可解群的子群是可解群，

(2)可解群的商群是可解群，

(3)令 G 是群， H 是 G 的正规子群，若 $H, G/H$ 都是可解群，则 G 是可解群，

证: (1)设 G 是可解群， H 是它的子群，有 $H^{(k)}$ 包含于 $G^{(k)}$

因此，若 $G^{(n)}=\{1\}$ ，则有 $H^{(n)}=\{1\}$ ，即 H 是可解群，

(2)令 G 是可解群， H 是它的正规子群，考察群的自然同态 $\pi: G \rightarrow G/H$ ，

对 n 使用数学归纳法可以证明 $(G/H)^{(n)}=\pi(G^{(n)})$

因此，若 G 是可解群，使得 $G^{(k)}=\{1\}$ ，

则 $(G/H)^{(k)}=\pi(G^{(k)})=\{1\}$ ，即商群 G/H 是可解群，

(3)因为 G/H 是可解群，所以存在正整数 k ，使得 $(G/H)^{(k)}=\{1\}$ ，

而在自然同态 $\pi: G \rightarrow G/H$ 下， $(G/H)^{(k)}=\pi(G^{(k)})$ ，

因此， $\pi(G^{(k)})=\{1\}$ ，即 $G^{(k)}$ 包含于 H ，

而 H 也是可解群，所以存在正整数 t ，使得 $H^{(t)}=\{1\}$ ，

再由 $G^{(k+t)}=(G^{(k)})^{(t)} \subseteq H^{(t)}=\{1\}$ 可知， G 是可解群，

我们已经知道交错群 $A_n(n \geq 5)$ 是非交换单群，因此， $A_n(n \geq 5)$ 不是可解群，

这必然导致对称群 $S_n(n \geq 5)$ 不是可解群(可解群的子群可解)，

令 G 是群，若存在 G 的子群列 $G=G_0 \supseteq G_1 \supseteq \cdots \supseteq G_{i-1} \supseteq G_i \supseteq \cdots$ (*)

使得 G_i 是 G_{i-1} 的正规子群， $i=1, 2, \cdots$ ，

则称(*)式是 G 的正规子群列，

定理 7.1 若 G 是群，则 G 是可解群的充分必要条件是

存在一个正规子群列 $G=G_0 \supseteq G_1 \supseteq \cdots \supseteq G_s=\{1\}$

使得商群 $G_{i-1}/G_i (1 \leq i \leq s)$ 是交换群，

证: 首先，若 G 是可解群，则由可解群的定义，知存在满足条件的正规子群列

其次，假设存在满足条件的正规子群列，

则需要指出，存在 k ，使得 $G^{(k)}=\{1\}$

为此，先证明对属于 N 的任意的 n ，有 $G^{(n)}$ 包含于 G_n

当 $n=0$ 时， $G^{(0)}=G=G_0$ ，即结论平凡成立，

当 $n=1$ 时，因为 G/G_1 是交换群，所以由命题 7.1(2) 可知， $G^{(n)}$ 包含于 G_1

假设 $G^{(n-1)}$ 包含于 G_{n-1} 成立，考察等于 n 的情况，

因为 G_{n-1}/G_n 是交换群，所以应用命题 7.1(2) 有 $[G_{n-1}, G_{n-1}]$ 包含于 G_n

从而 $G^{(n)}=[G^{(n-1)}, G^{(n-1)}] \subseteq [G_{n-1}, G_{n-1}] \subseteq G_n$

因此，由数学归纳法可知，对属于 N 的任意的 n ，总有 $G^{(n)}$ 包含于 G_n

最后，因为 $G_s=\{1\}$ ，所以 $G^{(s)}$ 包含于 $G_s=\{1\}$ ， $G^{(s)}=\{1\}$ ，即 G 是可解群

引理 7.1 不等于 $\{1\}$ 的有限交换单群 H 是素数阶的，

证: 因为交换群的子群是正规子群，所以若 H 是交换单群，

则 H 的子群都是平凡子群，

因而对属于 H 的任意 x ，有 $\langle x \rangle = H$ ，即 H 是循环群，其中 x 不为 1 ，

若素数 p 是 $|H|$ 的因子，则由第二章定理 5.4 可知， H 有 p 阶子群，

这个 p 阶子群就是 H 本身，所以 H 是素数阶的，

定理 7.2 若 G 是有限群，则 G 是可解群的充分必要条件是存在正规子群列 $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_{s-1} \supseteq G_s = \{1\}$ ，使得商群 $G_{i-1}/G_i (1 \leq i \leq s)$ 是素数阶循环群，

证： 因为循环群是交换群，所以根据定理 7.1 可知充分性成立，

若 G 是可解群，则由定理 7.1 可知，存在一个正规子群列 $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_{s-1} \supseteq G_s = \{1\}$ ，使得 $G_{i-1}/G_i (1 \leq i \leq s)$ 是交换群

因此，我们只要证明通过加细一段，使之成为一个正规子群列，并且满足商群是素数阶群即可，

为此，令 N 是 G 的正规子群，并且， G/N 是交换群，

若 G/N 是单群，则由引理 7.1 可知， $|G/N|$ 是素数，

即此段已经加细成满足条件要求的子群列了，

如若不然，那么存在 G/N 的一个极大正规子群 $H/N (\neq G/N)$ ，使得 $(G/N)/(H/N)$ 是交换单群，

根据群的第二同构定理有 $(G/H) \cong (G/N)/(H/N)$ ，

因此，在正规子群列 $G \supseteq H \supseteq N$ 中， G/H 是交换单群，于是 $|G/H|$ 是素数，

我们可以利用同样的方法加细 $H \supseteq N$ 段，……

因为 G 是有限群，所以这种加细的过程一定能在有限步之内完成，

综上，如果群 G 是有限可解群，那么一定存在正规子群列 $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_{s-1} \supseteq G_s = \{1\}$ ，使得商群 $G_{i-1}/G_i (1 \leq i \leq s)$ 是素数阶循环群，

例 7.3 证明 p -群 G 是可解群，

证： 设 $|G| = p^n$ ，对 n 用数学归纳法，

当 $n=1$ 时， p 阶群是交换群，当然是可解群，

假设 $p^m (m < n)$ 阶群是可解群，下证 p^n 阶群是可解群

因为 p -群的中心是非平凡的，所以 $|G/C(G)| < p^n$

由归纳假设可知 $G/C(G)$ 是可解群，

从而根据命题 7.2(3) 推得 G 是可解群

例 7.4 令 p, q 是不同的素数，证明 pq 阶群是可解群，

证: 不妨假设 $p < q$ ，

若 G 是 pq 阶群，则由西罗定理可知， G 有西罗 q -子群，

若 G 有 k 个西罗 q -子群，则 $k \equiv 1 \pmod{q}$ 且 $k|p$ ，

因为 $p < q$ ，所以只能是 $k=1$ ，即群 G 只有一个西罗 q -子群，

设其为 H ，那么 H 是 G 的正规子群，

于是有下面的正规子群列 $G \supseteq H \supseteq \{1\}$ ，

因为 $|G/H|=p$ ， $|H/\{1\}|=q$ ，所以商群 $G/H, H/\{1\}$ 是素数阶循环群，

根据定理 7.2 可知， G 是可解群，

作为例 7.4 的一个直接推论，因为 $|S_3|=6=2 \times 3$ ，所以 S_3 是可解群，