所谓用根式解方程是指利用加、减、乘、除及开方运算，

将一个多项式的根用该多项式的系数表示出来，

早在 16 世纪，人们就已经给出了 3 次、4 次多项式方程的根式解，

但直到 19 世纪 30 年代，更高次方程的求解问题才由数学家伽罗瓦解决，

本节简单论述无重根多项式的根式解

与根式扩张及多项式的伽罗瓦群之间的关系，

假定这节涉及的域均是特征为 0 的域，且包含所有 n 次单位根，

设 $f(x)$是 $F[x]$中的多项式，

若考虑 $f(x)$的根能否用加、减、乘、除及开方 Q 运算表示出来，

则仅需考察域 F 中元素的方根，

实际上，属于 F 的 a 的 n 次方根是多项式 $g(x)=x^n-a$ 的根，

若α是 $g(x)$的一个 n 次方根，则$\alpha, \alpha\theta, \cdots, \alpha\theta^{n-1}$是 $g(x)$的全部根，

(θ是本原 n 次单位根)，即 $F(\alpha)$是 $g(x)$在 F 上的分裂域，

因此，求 a 的 n 次方根，即是求包含 F 的正规扩张 $F(\alpha)$

(这样的扩张称为单根式扩张)，

又若 n 不是素数，则 $n=pq, g(x)=(x^q)^p-a$，那么求 $g(x)$的 n 次方根，等价于

先在 F 的基础上求 p 次方根α_1，得到包含 F 的扩张 $F(\alpha_1)$，

再在 $F(\alpha_1)$的基础上求 q 次方根α_2，得到包含 $F(\alpha_1)(\alpha_2)$的扩张 $F(\alpha_1)$，

因此，仅需要讨论清楚开素数次方根的情况即可，

定义 8.1 令包含 F 的 E 是域的扩张，

若存在中间域 $F_i(0\leqslant i\leqslant m)$，使得 $F=F_0\subseteq F_1\subseteq F_2\subseteq\cdots\subseteq F_{m-1}\subseteq F_m=E$ (1)

其中 $F_i=F_{i-1}(\alpha_i)$，$\alpha_i^{p_i}$属于 F_{i-1}，$1\leqslant i\leqslant m$，p_i 是素数，

则称 E 是 F 的根式扩张，(1)式称为 E 对 F 的根式扩张链，

显然，如果一个多项式的根能够用加、减、乘、除及开方运算表示出来，

那么该根一定属于某个根式扩张链的一个中间域，

反之，一个元素属于某个根式扩张链的一个中间域，

则它一定可以用加、减、乘、除及开方运算表示出来

定义 8.2 设 F 是域 f(x)属于 F[x]，

若有 F 的根式扩张 E 包含 f(x)的分裂域，则称 f(x)在 F 上可以用根式解，

下面我们将简述属于 F[x]的 f(x)可以用根式解

与 f(x)的伽罗瓦群(f(x)的分裂域 E 关于 F 的伽罗瓦群)之间的关系，

定理 8.1 设 f(x)属于 F[x]，若 f(x)在 F 上的分裂域为 E，

则$|Aut_FE|=|E:F|$，且包含 F 的 E 是有限伽罗瓦扩张，

证: 因为包含 F 的 E 是有限扩张，

所以由本章推论 3.2 可知，包含 F 的 E 是单代数扩张，

若设 $E=F(\alpha)$，α在 F 上的极小多项式为 g(x)，

则 Aut_FE 中的任意元素σ由$\sigma(\alpha)$决定，且$\sigma(\alpha)$是 g(x)的根，

由本章定理 4.3 可知，包含 F 的 E 是正规扩张，进而 g(x)的根都属于 E，

因此，$|Aut_FE|$等于 g(x)的不同根的个数，

由第三章推论 9.2 可知，g(x)没有重根，所以，$|Aut_FE|=\deg g(x)=|E:F|$，

因为 F 包含于 F"，所以 E 是 f(x)在 F"上的分裂域，因此，$\left|Aut_{F''}E\right|=|E:F|$，

再由$Aut_{F''}E=Aut_FE$ 及$|E:F|=|E:F''||F'':F|$可得$|F'':F|=1$，即 F=F"

从而，包含 F 的 E 是伽罗瓦扩张

由本章定理 8.1、定理 4.3 和命题 6.3，我们有下面的推论 8.1，

推论 8.1 包含 F 的 E 是有限伽罗瓦扩张的充分必要条件是包含 F 的 E 是正规扩张

引理 8.1 若 E 是 F 的一个根式扩张，则存在 F 的一个根式扩张 L

使得包含 F 的 L 是正规扩张，且 E 是包含 F 的 L 的中间域

证: 令 F 的任意一个根式扩张 E 为 $F=F_0\subseteq F_1\subseteq F_2\subseteq\cdots\subseteq F_{m-1}\subseteq F_m=E$

其中 $F_i=F_{i-1}(\alpha_i)$，α_i 是属于 $F_{i-1}[x]$的$x^{p_i}-a_i$ 的根，p_i 是素数，

首先，因为所有本原 p_i 次单位根属于 F，

所以属于 F[x]的 $f_1(x)=x^{p_1}-a_1$ 的所有根属于 $F_1=F_0(\alpha_1)$

即 F_1 是 $f_1(x)$的分裂域，进而包含 F_0 的 F_1 是正规扩张，若 $E=F_1$，则结论证毕，

如若不然，则 F_1 包含于 E，$F_1\neq E$，此时，因为 $F_2=F_1(\alpha_2)$，

所以我们可以构造一个F_1上的属于$F_1[x]$的多项式$f_2(x)=\prod_{\sigma}\left(x^{p_2}-\sigma(a_2)\right)$

这里的σ是 F_1 关于 F 的伽罗瓦群中的元素，

因为 $f_2(x)$的系数在所有 F_1 关于 F 的伽罗瓦群中元素的作用下保持不变，

所以 $f_2(x)$属于 F[x]，

现在，我们把 $f_2(x)$的根添加到 F_1 上，得到 F_2 的扩张 E_2

因为 F 包含本原 p_2 次单位根，

所以 E_2 是属于 F[x]的多项式 $f_1(x)f_2(x)$的分裂域，进而是 F 的正规扩张，

若 E 包含于 E_2，则 E_2 就是所求的 K，否则，F_2 包含于 E，$F_2\neq E$

因为 $F_3=F_2(\alpha_2)$，

所以我们可以构造一个E_2上的属于$E_2[x]$的多项式$f_3(x)=\prod_{\sigma}\left(x^{p_3}-\sigma(a_3)\right)$

这里的σ是 E_2 关于 F 的伽罗瓦群中的元素，

因为 $f_3(x)$的系数在所有 E_2 关于 F 的伽罗瓦群中元素的作用下保持不变

所以 $f_3(x)$属于 F(x)，

继续使用上面的构造过程，得到 E_3 是属于 F[x]的多项式 $f_1(x)f_2(x)f_3(x)$的分裂域

进而 E_3 是 F 的正规扩张，

如果 E 包含于 E_3，则 E_3 就是所求的 K，

否则，按同样的过程，经过有限次步骤后，一定可以得到F的一个根式扩张K，

使得包含 F 的 K 是正规扩张，且 E 是包含 F 的 K 的中间域，

定理 8.2 若属于 F[x]的 f(x)在 F 上可以用根式解，则 f(x)的伽罗瓦群是可解群，

证: 设 E 是 f(x)在 F 上的分裂域，

因为 f(x)可以用根式解，所以 E 是 F 的根式扩张链中的一个中间域，

进而由引理 8.1 可知，

存在包含 F 的正规根式扩张 L，使得 E 是包含 F 的 L 的中间域，

设 L 对 F 的根式扩张链为 $F=F_0\subseteq F_1\subseteq\cdots\subseteq F_m=L$，

其中 $F_i=F_{i-1}(\alpha)$，$\alpha_i^{p_i}$属于 F_{i-1}，$1\leqslant i\leqslant m$，p_i 是素数，

由推论 4.2 可知，包含 F_i 的 L 是正规扩张，

令 L 关于 F 的伽罗瓦群为 G，则有 $G=G_0\supseteq F_1'\supseteq F_2'\supseteq\cdots\supseteq F_m'=\{1\}$，其中$F_i'=Aut_{F_i}L$

根据定理 8.1 和推论 8.1 可知，包含 F_{i-1} 的 F_i 是正规扩张，

根据本章理 6.2(3)可知，F_i'是F_{i-1}'的正规子群，且$F_{i-1}'/F_i'\cong Aut_{F_{i-1}}F_i$

再由$|Aut_{F_{i-1}}F_i|=|F_i:F_{i-1}|=p_i$，可知，$F_{i-1}'/F_i'$是素数阶循环群，

因此，由本章定理 7.2 可知 $G=Aut_FL$ 是可解群，

现在，需要指出 Aut_FE 是可解群，

因为 $L\supseteq E\supseteq F$ 且 E 是 F 的正规扩张，

所以由本章定理 6.2 可知 $Aut_FE\cong Aut_FL/Aut_FL$

因为可解群的商群是可解群，所以 Aut_FE 是可解群，

引理 8.2 设包含 F 的 E 是伽罗瓦扩张，

若$|E:F|=p$(p 是素数)，则存在属于 E 的δ，使得 $E=F(\delta)$且δ^p 属于 F，

证: 因为$|E:F|=p$ 是素数，所以对属于 E\F 的任意 b，都有 $E=F(b)$，

又由本章定理 6.2(2)可知 Aut_FE 是 p 阶循环群，

令 $Aut_FE=\langle\sigma\rangle$，则由 $E=F(b)$可知，σ由$\sigma(b)$决定，

令 $A=(a_{ij})$，$a_{ij}=(\sigma^{j-1}(b))^{i-1}$，$i,j=1,2,\cdots,p$，则 $\det(A)\neq0$，

设θ是本原 p 次单位根，$x=(1,\theta,\cdots,\theta^{p-1})^T$，则 $Ax\neq0$，

从而,存在 i 使得$\delta=\sum_{j=0}^{p-1}\sigma^j(b^{i-1})\theta^j=0$

于是有$\sigma(\delta)=\sum_{j=0}^{p-1}\sigma^{j+1}(b^{i-1})\theta^j=\sum_{j=0}^{p-1}\sigma^{j+1}(b^{i-1})\theta^{j+1}\theta^{-1}$

$=\sum_{j=0}^{p}\sigma^j(b^{i-1})\theta^j\theta^{-1}=\sum_{j=0}^{p-1}\sigma^j(b^{i-1})\theta^j\theta^{-1}=\delta\theta^{-1}$

从而$\sigma(\delta^p)=\sigma(\delta)^p=(\delta\theta^{-1})^p=\delta^p$，即对属于 Aut_FE 的任意τ，都有$\tau(\delta^p)=\delta^p$

这说明δ^p 属于$(Aut_FE)'=F$

下面验证δ不属于 F，

若δ属于 F，则$\sigma(\delta)=\delta$，再由$\sigma(\delta)=\delta\theta^{-1}$，得$\theta=1$，这与$\theta$是本原 p 次单位根矛盾，

因此，δ不属于 F，$E=F(\delta)$，δ^p 属于 F，

定理 8.3 若属于 F[x]的 f(x)的伽罗瓦群 G 是可解群，则 f(x)在 F 上可以用根式解

证: 设 E 是 f(x)在 F 上的分裂域，因为 G 是有限可解群，

所以存在正规子群列 $G=G_0\supseteq G_1\supseteq G_2\supseteq\cdots\supseteq G_m=\{1\}$使得 G_i 是 G_{i-1} 的正规子群，

并且$|G_{i-1}/G_i|=p_i$，其中 p_i 是素数，

那么对应有 E 与 F 的中间域序列 $F=G_0'\subseteq G_1'\subseteq G_2'\subseteq\cdots\subseteq G_m'=E$，

因为包含 F 的 E 是有限伽罗瓦扩张，从而是正规扩张，

所以根据本章推论 4.2 可得包含G_i'的 E 是正规扩张，

因为G_i是G_{i-1}的正规子群，所以由本章定理 6.2(2)可知包含G_i'的G_{i+1}'是正规扩张

又由$|G_i' : G_{i-1}'|=|G_{i-1} : G_i|=p_i$及引理 8.2 可知

存在$\alpha_i(1\leqslant i\leqslant m)$使得$G_i'=G_{i-1}'(\alpha_i)$，其中$\alpha_i^{p_i}$属于$G_{i-1}'$

所以，E 是 F 的根式扩张，即多项式 f(x)能用根式求解

至此，

我们得到多项式能用根式解的充分必要条件是该多项式的伽罗瓦群是可解群，

设 f(x)是 F[x]中 n 次多项式，且 f(x)没有重根，

E 是 f(x)在 F 上的分裂域，$\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 f(x)的 n 个根，

则对属于 Aut_FE 的σ，有$\sigma(\alpha_1),\sigma(\alpha_2),\cdots,\sigma(\alpha_n)$恰为 f(x)的 n 个不同根，

即存在置换$\sigma(f(x))=\begin{pmatrix}\alpha_1 & \alpha_2 & \cdots & \alpha_n\\ \sigma(\alpha_1) & \sigma(\alpha_2) & \cdots & \sigma(\alpha_n)\end{pmatrix}$

从而有 Aut_FE 到 S_n 的单同态$\rho : Aut_FE\to S_n,\sigma\to\sigma(f(x))$

因此，一个多项式的伽罗瓦群可以看做是对称群 S_n 的子群，

然而我们知道，对于对称群 S_n，当 $n\leqslant 4$ 时，对称群 S_n 及其子群是可解群，

当 $n\geqslant 5$ 时，对称群 S_n 不是可解群，

所以，我们得到阿贝尔定理，

定理 8.4(阿贝尔)当 $n\geqslant 5$ 时，一般 n 次多项式不能用根式解，

本节最后，我们再简单说明的确存在不能用根式求解的多项式方程，

为此，给出下面的命题，这里略去证明过程，

命题 8.1 令属于 Q[x]的 f(x)是 p 次(p 为素数)不可约元，

若 f(x)恰好有两个复数根，则 f(x)的伽罗瓦群是对称群 S_p

例 8.1 令 $f(x)=2x^5-5x^4+5$ 属于 Q[x]，则由艾森斯坦判别法，f(x)是不可约元，

利用微积分的方法，我们可知它有 3 个实数根，

所以，f(x)的伽罗瓦群 G 是对称群 S_5

但是 S_5 不是可解群，因此，f(x)不能用根式解