5. Sufficient & necessary conditions for solving algebraic equation

Recall the quadratic equation $x^2+ax+b=0$, which can be viewed as defined on $F=Q(a,b)$. Add $\sqrt{\Delta}=\sqrt{a^2-4b}$ into F. We arrive at the extended field $F(\sqrt{\Delta})$, which includes the roots $\frac{1}{2}(-a\pm\sqrt{\Delta})$. For high order equations, consider the one below defined on $F=Q(a_1,\cdots a_n)$,

$$X^n+a_1X^{n-1}+\cdots+a_{n-1}X+a_n=0.$$

✡ Whether it can be solved by the radical method is equivilent to whether we can start with F by adding radical expressions one by one to extend F, and finially reach the root field N. The extended field K_i form a series of middle fields between F and N, i.e.

$$\boxed{F=K_0\subset K_1\subset K_2\cdots\subset K_S=N.} \quad (*)$$

Here every $K_{i+1}=K_i(\alpha_i^{1/r_i})$ with $\alpha_i\in K_i$ but $\sqrt[r_i]{\alpha_i}\notin K_i$. Without loss of generality, we assum that r_i is a prime number, otherwise, we can factorize it and repeat the above process. (If $r=st$, we can first add $\alpha^{1/s}$ to form $K_i(\alpha^{1/s})$, and then add $(\alpha^{1/s})^{1/t}$ to form $K_{i+1}=K_{i+2}=K_{i+1}((\alpha^{1/s})^{1/t})$.) Another minor thing is that we assume that F, i.e, K_0 already contains all the unit roots at arbitary orders. (All unit roots can be obtained by algebraic method, and this does not brings any difficult. For simplicity, we still call this field as F.

We know that the roots of $x^{r_i} = \alpha_i$ including α_i^{1/r_i}, $\alpha_i^{1/r_i}\xi$, $\cdots \alpha_i^{1/r_i}\xi^{r_i-1}$

They all belong to K_{i+1}, hence, it is a normal extension to K_i. As shown before $Gal(K_{i+1}/K_i)$ is a r_i-th order cyclic group, hence, it is a cyclic extension of fields. Similarly, all the field extensions in (*) are normal extensions. Moreover, the ratios of dimensions are all prime.

We can derive the Galois groups:

$G_0 = Gal(N/K_0)$, $G_1 = Gal(N/K_1)$, $\cdots G_{s-1} = Gal(N/K_{s-1})$, $\cdots G_s = \{(e)\} = Gal(N/N$

Since all extensions are normal, G_i is a normal subgroup of G_{i+1}. They form a composite sequence

Cyclic extension

$$G_0 \triangleright G_1 \triangleright G_2 \cdots \triangleright \{e\}.$$

↓

And $G_i/G_{i+1} = Gal(N/K_i)/Gal(N/K_{i+1}) = Gal(K_{i+1}/K_i) = C_{r_{i+1}}$

Hence, if an equation can be solved algebracially,

its Galois group over $F(a_1, \cdots a_n)$ must be a solvable group,

↑

$Gal(N/F)$

✡ Now let us look the sufficiency: Consider a special case

$X^n + a_1 X^{n-1} + \cdots a_n = 0$, $n = p$ is a prime #.

And its Galois group is the p-th cyclic group generated by $a = \begin{pmatrix} 1 & 2 & \cdots & n \\ 2 & 3 & \cdots & 1 \end{pmatrix}$

$G = \{ I, a, a^2, \cdots a^{n-1} \}$.

Assume its roots $x_1, x_2, \cdots x_n$, set $\xi = e^{i\frac{2\pi}{n}}$.

$$\begin{cases} x_1 + x_2 + \cdots x_n = r_0 = -a_1 \in F \\ x_1 + \xi x_2 + \cdots \xi^{n-1} x_n = r_1 \\ \vdots \\ x_1 + \xi^{n-1} x_2 + \cdots \xi^{(n-1)(n-1)} x_n = r_{n-1} \end{cases}$$

Look at the 2nd Eq, apply $\begin{pmatrix} 1 & 2 & \cdots & n \\ 2 & 3 & \cdots & 1 \end{pmatrix} \Rightarrow x_2 + \xi x_3 + \cdots \xi^{n-1} x_1 = a(r_1)$

$\Rightarrow \xi^{n-1}(x_1 + \xi x_2 + \cdots \xi^{n-1} x_n) = \xi^{n-1} r_1 = a(r_1)$

Similarly, we arrive the mapping $\boxed{a(r_k) = \xi^{-k} r_k, \quad k = 1, 2, \cdots n-1.}$

Hence $a(r_k^n) = a(r_k) \cdots a(r_k) = \xi^{-nk} r_k^n = r_k^n$, hence $r_k^n \in F$.

In other words, we can find a number in F, which is a function of the coefficients, denoted as α_k. Then $r_k = \sqrt[n]{\alpha_k}$, and we adel them ($k = 1, \cdots n-1$) into F. Hence, we only need to solve linear equations based on $\xi^1, \cdots \xi^{n-1}, \sqrt[n]{\alpha_1}, \cdots \sqrt[n]{\alpha_k}$ to solve the equation.

For the general case, if Gal(N/F) is solvable, we have the composite sequence.

$$G_0 = Gal(N/K_0) \triangleright G_1 \cdots \triangleright G_i \triangleright G_{i+1} \cdots \triangleright G_s = \{e\}$$

$$K_0 \longrightarrow K_1 \cdots K_i \longrightarrow K_{i+1} \rightarrow \cdots N$$

Consider $G_{i+1}/G_i = C_{r_{i+1}}$ ← prime # order cyclic group.

Correspondingly, we can extend $K_i \longrightarrow K_{i+1}$, such that $\mathrm{Gal}(K_{i+1}/K_i)$

$$= \left\{ I,\ \tau = \begin{pmatrix} 1 & 2 & \cdots & r_{i+1} \\ 2 & 3 & \cdots & 1 \end{pmatrix},\ \tau^2,\ \cdots\ \tau^{r_{i+1}-1} \right\}.$$

Since K_{i+1} is a normal extension to K_i, then K_{i+1} is the root field of an equation $P_i(x) = 0$ defined on K_i. Since its Galois group $\mathrm{Gal}(K_{i+1}/K_i)$ is the p-th cyclic group, according to the result in the last page, $P_i(x) = 0$ can be solved algebracially. Hence, #'s in K_{i+1} can be obtained via $+ - \times \div \sqrt[r]{\ }$ based on K_i. Hence, #'s in the root field N, can be obtained algebracially from F.

✱ Algebracal Solution to the cubic equation — Cardano formula

Consider $x^3+px+q=0$ defined on $K_0=\mathbb{Q}(p,q,\omega)$

Since for a general (set) coefficients, $Gal[N/K_0]=S_3$. It is not a cyclic group, but solvable. We design the composite sequence

$$\begin{array}{ccccc} S_3 & \triangleright & C_3 & \triangleright & \{e\} \\ \downarrow & & \downarrow & & \downarrow \\ K_0 & \xrightarrow{2} & K_1 & \xrightarrow{3} & N \\ \| & & & & \\ \mathbb{Q}(p,q) & & & & \end{array}$$

① Since $\sqrt{d}=(x_1-x_2)(x_2-x_3)(x_3-x_1)$ is generally not in K_0, we need to add it to K_0

$K_1=K_0(\sqrt{d})$, where $d=4p^3+27q^2$.

② $N=K(x_1,x_2,x_3,\omega)$ and N/K_1 is 3-cyclic extension. $Gal[N/K_1]=C_3$. We consider $\sigma\in Gal(N/K_1)$, and

$\sigma(x_1)=x_2,\ \sigma(x_2)=x_3,\ \sigma(x_3)=x_1$.

Define $\begin{cases} x_1+\omega x_2+\omega^2 x_3=A \\ x_1+\omega^2 x_2+\omega x_3=B \\ x_1+x_2+x_3=0 \end{cases}$

According to the results before, we have A^3 and $B^3\in K_0$.

$$A^3+B^3=(A+B)(A^2+B^2-AB)=(A+B)((A+B)^2-3AB)$$

$$A\cdot B=x_1^2+x_2^2+x_3^2+(\omega+\omega^2)(x_1x_2+x_2x_3+x_3x_1)$$
$$=(x_1+x_2+x_3)^2-3(x_1x_2+x_2x_3+x_3x_1)=-3p \Rightarrow A^3B^3=-27p^3$$

$$A^3+B^3=(A+B)(A^2+B^2-AB)=(A+B)^3-3(A+B)AB=27(x_1^3+px_1)=-27q$$

$$\Rightarrow\quad y^2+27qy-27p^3=0 \qquad \Delta=(27q)^2+4\cdot 27p^3=$$

$$A^3,B^3=\frac{1}{2}\left[-27q\pm\sqrt{(27q)^2+4\cdot 27p^3}\right]$$

$A^3, B^3 = 27\left(-\frac{q}{2} \pm \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}\right) \in K_1 = K_0(\sqrt{d})$

adel square root

$u, v = \frac{A}{3}, \frac{B}{3} = \left(-\frac{q}{2} \pm \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}\right)^{1/3} \in N = K_1(A, B)$

adel cubic root

then
$$\begin{cases} x_1 = u + v \\ x_2 = u\omega + v\omega^2 \\ x_3 = u\omega^2 + v\omega \end{cases}$$

Comment: ① when $\Delta = (\frac{q}{2})^2 + (\frac{p}{3})^3 < 0$, u and v are a pair of conjugate complex numbers. $\Rightarrow$ x_1, x_2, x_3 are real roots. On the contary, if $\Delta > 0$, then we take u and v as real, but with different magnitude, then x_1 is real, but x_2 and x_3 are complex and conjugate to each other.

② In the case of $\Delta < 0$, we need to involve complex # to reach real roots of a real equation!

Then can we find a purely real radical formula to solve the cubic equation when $\Delta < 0$? The answer is no!

Theorem: If a real coefficient equation $y^3 + py + q = 0$ has all the three roots real, and its irreducible on the field F of its coefficient, then there does not exist a radical formula only containing real radical expressions.

Proof: We denote $D=[(y_1-y_2)(y_2-y_3)(y_3-y_1)]^2=-108\Delta>0$. If we only add $\sqrt{D}$ to F, then $F(\sqrt{D})$ is a 2nd order extension, but $Gal(N/F)=S_3$. (N is the root field.)
This is not enough!

Consider N can be extended via adding real radical expressions

$$F(\sqrt{D}) \subset K_1 \subset K_2 \cdots \subset K_s = N, \quad \text{where } K_{i+1}=K_i(a_i^{1/r_i})$$

with $a_i \in K_i$, r_i prime #. Pick up, any root y_1. $y_1 \notin F(\sqrt{D})$, otherwise we can show (see later) $N=F(\sqrt{D}, y_1)$. Then assume $y_1 \in K_{i+1}$, but y_1 is not in K_i, then K_{i+1} must include y_2 and y_3, hence $N=K_{i+1}$.

Hence K_{i+1} is the root field of $y^3+py+q=0$, and must be a normal field. Since $\sqrt[3]{\alpha_i} \in K_{i+1}$, then K_{i+1} must include all the three roots of $x^3=\alpha_i$, i.e $\sqrt[3]{\alpha_i}\,\omega$ and $\sqrt[3]{\alpha_i}\,\omega^2$. Hence K_{j+1} cannot be a real field!

* Now we prove that $N=F(\sqrt{D}, y_1)$.

Proof: Since $\sqrt{D} \in N$, $y_1 \in N$, we have $F(\sqrt{D}, y_1) \subseteq N$. We only need to prove y_2 and y_3 also $\in F(\sqrt{D}, y_1)$. Consider $(y_1-y_2)(y_1-y_3)=y_1^2-(y_2+y_3)y_1+y_2y_3$,

$$=y_1^2+y_1^2-(-y_1)y_1+q/y_1$$

then $(y_1-y_2)(y_1-y_3) \in F(\sqrt{D}, y_2)$.

Hence $y_2-y_3=\dfrac{\sqrt{D}}{(y_1-y_2)(y_1-y_3)} \in F(\sqrt{D}, y_1)$, also $y_2+y_3=-y_1$,

we have $y_{2,3}$ also $\in F(\sqrt{D}, y_1)$.

★ Algebraic solution to the quartic equation

Consider $x^4 + px^2 + qx + r = 0$ defined on a field F. Its Galois group $\mathrm{Gal}(N/F) = S_4$. The composite group sequence is

$$\begin{array}{ccccccccc} S_4 & \triangleright & A_4 & \triangleright & D_2 & \triangleright & C_2 & \triangleright & \{e\} \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ F & \xrightarrow{2} & F(\sqrt{D}) & \subset^{3} & \Lambda_1 & \subset^{2} & \Lambda_2 & \subset^{2} & N \end{array}$$

① $F \to F(\sqrt{D})$ is standard, which is a square root extension by adding $\sqrt{D}$. Then $\mathrm{Gal}(N/F(\sqrt{D})) = A_4$. ($\sqrt{D}$ is invariant under even permutation

② $F(\sqrt{D}) \to \Lambda_1$ is a cubic extension. The extended field Λ_1 should be invariant under $D_2 = \{e, (12)(34), (13)(24), (14)(23)\}$

we construct
$$\begin{cases} \theta_1 = (x_1 + x_2)(x_3 + x_4) \\ \theta_2 = (x_1 + x_3)(x_2 + x_4) \\ \theta_3 = (x_1 + x_4)(x_2 + x_3) \end{cases}$$

$\theta_{1,2,3} \notin F(\sqrt{D})$, but they are invaraint under D_2

$\Rightarrow \Lambda_1 = F(\sqrt{D}, \theta_1, \theta_2, \theta_3)$

$\theta_{1,2,3} \notin F(\sqrt{D})$, but they should satisfy an equation on $F(\sqrt{D})$. Consider

$$\begin{aligned} f(\theta) &= (\theta - \theta_1)(\theta - \theta_2)(\theta - \theta_3) \\ &= \theta^3 - (\theta_1 + \theta_2 + \theta_3)\theta^2 + (\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1)\theta - \theta_1\theta_2\theta_3 \end{aligned}$$

$\theta_1 + \theta_2 + \theta_3$, $\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1$, $\theta_1\theta_2\theta_3$ are invarant under $S_4/D_2 = S_3$.

$$\begin{cases} \theta_1 + \theta_2 + \theta_3 = 2(x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4) = 2p \\ \theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1 = p^2 - 4r \\ \theta_1\theta_2\theta_3 = -q^2 \end{cases}$$

This is a cubic equation

$f(\theta) = \theta^3 - 2p\theta^2 + (p^2-4r)\theta + q^2$, which can be solved by adding cubic roots into $F(\sqrt{D})$, and that is $F(\sqrt{D}, \theta_1, \theta_2, \theta_3) = \Lambda_1$

② $\Lambda_1 \to \Lambda_2$ is again a square root extension by adding $\sqrt{-\theta_1}$. Then $\Lambda_2 = \Lambda_1(\sqrt{-\theta_1})$,

$\sqrt{-\theta_1}$ is invariant under $\{e, (12)(34)\} = C_2$.

④ The last step extenstion $\Lambda_2 \to N$ is again a square root extension by adding $\sqrt{-\theta_2}$. Then we do not have non-trival symmetries since only $\{e\}$ can leave $\begin{cases} x_1+x_2 = \sqrt{-\theta_1} \\ x_1+x_3 = \sqrt{-\theta_2} \end{cases}$ both invariant!

Actually, we have already arrived the root field since $(-\theta_1)(-\theta_2)(-\theta_3) = q^2$

$\Rightarrow \sqrt{-\theta_3} = q / \sqrt{-\theta_1} \cdot \sqrt{-\theta_2}$, which is also in

$N = F(\sqrt{D}, \theta_{1,2,3}, \sqrt{-\theta_1}, \sqrt{-\theta_2})$

With all these extensions, we have

$(x_1+x_2)(x_3+x_4) = \theta_1 \Rightarrow \alpha_1 = x_1+x_2 = \pm\sqrt{-\theta_1}$

$(x_1+x_3)(x_2+x_4) = \theta_2 \quad \alpha_2 = x_1+x_3 = \pm\sqrt{-\theta_2}$

$(x_1+x_4)(x_2+x_3) = \theta_3 \quad \alpha_3 = x_1+x_4 = \pm\sqrt{-\theta_3}$

Since $(x_1+x_2)(x_1+x_3)(x_1+x_4) = x_1^2(x_1+x_2+x_3+x_4) + (x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4)$

$= -q.$

we should choose the signs of $\alpha_{1,2,3}$ consistent with the above.

$$\Rightarrow \quad 2x_1 = x_1+x_2 + x_1+x_3 + x_1+x_4$$
$$2x_2 = x_1+x_2 + x_2+x_4 + x_2+x_3$$
$$2x_3 = x_3+x_4 + x_1+x_3 + x_2+x_3$$
$$2x_4 = x_3+x_4 + x_2+x_4 + x_1+x_4$$

$$\Rightarrow$$

$$x_1 = \tfrac{1}{2}(\alpha_1+\alpha_2+\alpha_3)$$
$$x_2 = \tfrac{1}{2}(\alpha_1-\alpha_2-\alpha_3)$$
$$x_3 = \tfrac{1}{2}(-\alpha_1+\alpha_2-\alpha_3)$$
$$x_4 = \tfrac{1}{2}(-\alpha_1-\alpha_2+\alpha_3)$$