12 March 2016

Cubic and quadric equations; Galois theory for pedestrians

H.M. Khudaverdian

This étude is written on the base of the book of A. Khovansky "Galois Theory" and it is inspired by the lecture 'Galois Lecture' for students on 2-nd march 2016 and by the discussion with R. Mkrtchyan in December 2015 of quantum mechanical interpretation of roots of Lie algebra,

The content of this étude is the following: Let H be an abelian normal subgroup of group S_n of permutations of n elements. (Instead S_n one may consider an arbitrary Galois group G, but for clarity we consider just a group S_n.) We suppose that S_n acts on the space of polynomials $\Sigma^{(n)}$ of n variables $x_1, x_2, \dots, x_n$.)

$$\Sigma^{(n)} = \mathbf{C}[x_1, \dots, x_n]\,.$$

Then we can perform the following constructions.

Consider an arbitrary element $h \in H$ of this group. The corresponding linear operator acting on space $\Sigma^{(n)}$ is diagonalisable, since $h^N = 1$. Moreover all elements of the group H can be diagonalised simultaneously since H is an abelian group. More precisely this means that one can consider the decomposition of space $\Sigma = \Sigma^{(n)}$ of polynomials on n variables on linear subspaces over characters of group H:

$$\Sigma = \oplus_{\lambda \in \hat{H}} \Sigma^{(n)}_\lambda$$

such that if $\lambda \in \hat{H}$ is an arbitrary character of H, then an arbitrary polynomial $P \in \Sigma^{(n)}_\lambda$ is an eignevector of all elements of h with eigenvalues $\lambda(h)$,

$$hP = \lambda(h) P\,.$$

(Here $\hat{H}$ is a dual group of group H. it is a group of characters of group H [1)]). One can say that all elements of group H are commuting observables, and they are simultaneously measurable.

Denote by $\Sigma^{(n)}_H$ the subspace of H-invariant polynomials (this is subspace corresponding to character $\lambda \equiv 1$.). All characters are taking values in roots of unity, i.e. for an arbitrary polynomial $P \in \Sigma^{(n)}_\lambda$, there exists an integer N such that the polynomial P^N belongs to the space Σ_H. Thus we come to conclusion:

An arbitrary polynomial in $\Sigma^{(n)}$ is a sum of roots of polynomials in Σ_H.

[1)] Groups $\hat{H}$ and H are both abelian groups with same numebr of elements, but in general they *are not isomorphic.*

Now concetrate on the question how to calculate H-invariant polynomials, ie. polybnomials in Σ_H.

Now suppose that H is an invariant subgroup in group S_n. In this case the smaller group $S_n \backslash H$ acts on the space Σ_H, i.e. H-invariant polynomials are roots of polynomial with smaller Galois group; if S_n is Galois group of initial polynbomial, then Galois group acting on H-invariant polynomials becomes $G = S_n \backslash H$. These considerations explain why if Galois group is solvable, then the roots of polynomial are expressed by taking operation of roots[2]. In particular for $n = 2, 3, 4$ symmetric groups (groups of all permutations) S_2, S_3, S_4 are solvable [3]. We come to the formulae which express polynomials in S_n via S_n-invariant polynomials for $n = 2, 3, 4$, i.e., solving cubic and quartic equations in radicals.

We will perform the scheme described above for quadratic, cubic and quatric polynomials.

quadratic equation $n = 2$

Group S_2 is abelian $S_2 = \{1, \sigma\}$, $\sigma^2 = 1$. It has two characters:

$$\begin{array}{cc} & \lambda_I \equiv 1 \\ \lambda_{II}\colon & \lambda_I(1) = 1\,, \lambda_{II}(\sigma) = -1 \end{array}\,, \quad \hat{S}_2 = \{\lambda_I, \lambda_{II}\}\,.$$

For an arbitrary polynomial $P \in \Sigma^{(2)}$, $P = P(x_1, x_2)$, we have

$$P = P_I + P_{II} = \underbrace{\frac{P + \sigma P}{2}}_{\text{even polynomial}} + \underbrace{\frac{P + \sigma P}{2}}_{\text{odd polynomial}}$$

$((\sigma P)(x_1, x_2) = P(x_2, x_1))$,

The decomposition of the space of polynomials is

$$\Sigma^{(2)} = \Sigma^{(2)}_{\lambda_I} + \Sigma^{(2)}_{\lambda_{II}}\,.$$

If $x_1 + x_2 = -p$, $x_1 x_2 = q$ (x_1, x_2 are roots of polynomial $x^2 + px + q$) then every even polynomial is S_2-invariant, i.e. it is polynomial on p, q. For every odd polynomial its square is S_2-invariant also, i.e. and odd polynomial is square root of polynomial on p, q. In particular for polynomial $P = x_1$ we have

$$x_1 = \frac{x_1 + x_2}{2} + \frac{x_1 - x_2}{2} = \frac{x_1 + x_2}{2} \pm \sqrt{\left(\frac{x_1 - x_2}{2}\right)^2} =$$

[2] here the word 'root' I use in two different meanings: 'root of polynomial' and 'operation of taking root'.

[3] The abelian group is solvable. The group G is solvable if it possesses abelian normal subgroup such that factor is solvable. In particular S_3 is solvable since $S_3 \backslash C_3 = S_2$ is abelian, where C_3 is cyclic subgroup. For S_4 one can consider abelian normal subgroup KI generated by permutations (12)(34) and (13)(24) (see details later in the text). The factor is group S_3. Hence $S - 4$ is solvable also.

$$\frac{x_1+x_2}{2} \pm \sqrt{\left(\frac{x_1+x_2}{2}\right)^2 - x_1x_2} = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q}\,.$$

Cubic equation $n = 3$

Group S_3 contains abelian normal subgroup $C_3 = \{1, s, s^2\}$, where $s = (123)$.

Abelian subgroup C_3 has following three characters:

$$\begin{array}{rl} & \lambda_0 \equiv 1 \\ \lambda_I: & \lambda_I(1) = 1\,, \lambda_I(s) = \varepsilon\,, \lambda_I(s^2) = \varepsilon^2 \\ \lambda_{II}: & \lambda_{II}(1) = 1\,, \lambda_{II}(s) = \varepsilon^2\,, \lambda_{II}(s^2) = \varepsilon \end{array} \quad , \quad \text{where } \varepsilon = e^{\frac{2\pi i}{3}}.\,, \quad ,$$

that is the group $\hat{C}_3$ of characters is $\hat{C}_3 = \{\lambda_0, \lambda_I, \lambda_{II}\}$.

For an arbitrary polynomial $P \in \Sigma^{(3)}$, $P = P(x_1, x_2, x_3)$ we have

$$P = P_0 + P_I + P_{II} = \underbrace{\frac{P + (sP) + (s^2P)}{3}}_{\text{eigenvalues } (1,1,1)} + \underbrace{\frac{P + \varepsilon^2(sP) + \varepsilon(s^2P)}{3}}_{\text{eigenvalues } (1,\varepsilon,\varepsilon^2)} + \underbrace{\frac{P + \varepsilon sP + \varepsilon^2(s^2P)}{3}}_{\text{eigenvalues } (1,\varepsilon^2,\varepsilon)}$$

In details: $(sP)(x_1, x_2, x_3) = P(x_2, x_3, x_1)$, the polynomials P_I, P_{II} are eigenvectors such that

$$sP_I = \lambda_I(s)P_I = \varepsilon P_I\,, s^2P_I = \lambda_I(s^2)P_I = \varepsilon^2 P_I$$
$$sP_{II} = \lambda_{II}(s)P_I = \varepsilon^2 P_{II}\,, s^2P_{II} = \lambda_{II}(s^2)P_{II} = \varepsilon P_{II}$$

The decomposition of spaces is:

$$\Sigma^{(3)} = \Sigma^{(3)}_{\lambda_0} + \Sigma^{(3)}_{\lambda_I} + \Sigma^{(3)}_{\lambda_{II}}\,.$$

The subspace Σ_{λ_0} is subspace of C_3-invariant polynomials.

The cube of every polynomial in $\Sigma^{(3)}_I$ or in $\Sigma^{(3)}_{II}$ is C_3-invariant polynomial. Hence every polynomial can be expressed via C_3-invariant polynomials with use of operation of taking cubic roots.

Now concetratae on C_3-invariant polynomials. On the space $\Sigma^{(3)}_{C_3}$ of C_3-invariant polynomials acts factor-group

$$S_3 \backslash C_3 = S_2$$

i.e. C_3 invariant polynomials are roots of quadratic equation!

Now if we consider polynomial $P = x_1$ we come to the formula for cubic roots.

Perform calulations

Suppose that $x_1 + x_2 + x_3 = -a$, $x_1x_2 + x_1x_3 + x_2x_3 = p$ and $x_1x_2x_3 = -q$ i.e. x_1, x_2, x_3 are roots of polynomial $x^3 + ax^2 + px + q$. According to decomposition formula we have:

$$x_1 = (x_1)_0 + (x_1)_I + (x_1)_{II} = \underbrace{\frac{x_1 + x_2 + x_3}{3}}_{\text{eigenvalue } 1} + \underbrace{\frac{x_1 + \varepsilon^2 x_2 + \varepsilon x_3}{3}}_{\text{eigenvalue } \varepsilon} + \underbrace{\frac{x_1 + \varepsilon x_2 + \varepsilon^2 x_3}{3}}_{\text{eigenvalue } \varepsilon^2} +$$

(We write down here eigenvalue of operator s.) The first expression is obviously not only C_3-invariant but it is S_3-invariant also: $(x_1)_0 = \frac{x_1+x_2+x_3}{3} = -\frac{a}{3}$. Later for simplicity without loss of generality we assume later than $a = x_1+x_2+x_3 = 0$ (changing $x_i \mapsto x_i - \frac{a}{3}$).

Denote $w_I = (x_1)_I$ and $w_{II} = (x_2)_{II}$. The cubes of expressions $w_I = (x_1)_I$ and $w_{II} = (x_2)_{II}$ are eigenvectors with eigenvalue 1, hence they are C_3-invariant. Hence the group $S_3 \backslash C_3 = S_2$ acts on these numbers, i.e. they are roots of quadratic equation: $[(12)]w_I^3 = w_{II}^3$.

C_3-invariant polynomails $w_I^3 + w_{II}^3$ and $w_I^3 w_{II}^3$ are invariant with respect to the action of factorgroup $S_2 = S_3 \backslash C_3$, i.e. these polynomials are S_3 invariant polynomials, i.e. they are expressed via coefficients: we have after long but simple calculations that

$$w_I^3 + w_{II}^3 = \left(\frac{x_1 + \varepsilon^2 x_2 + \varepsilon x_3}{3}\right)^3 + \left(\frac{x_1 + \varepsilon x_2 + \varepsilon^2 x_3}{3}\right)^3 = -q$$

and

$$w_I^3 \cdot w_{II}^3 = \left(\frac{x_1 + \varepsilon^2 x_2 + \varepsilon x_3}{3}\right)^3 \left(\frac{x_1 + \varepsilon x_2 + \varepsilon^2 x_3}{3}\right)^3 = -27p^6$$

Hence

$$x_1 = w_0 + w_I + w_{II} = \sqrt[3]{w_1} + \sqrt[3]{w_2} = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \qquad (\dagger)$$

Remark The question what branch of cubic root to choose can be answered if we note that $w_I w_{II}$ is S_3 invariant under the action of S_3.

Quartic equations $n = 4$

First explain why and how we choose ableian subbgroup in S_4.

Consider platonic body, tetrahedron $A_1A_2A_3A_4$. On vertices of this tetrahedron acts group S_4.

Let

E_1 be a middle point of the segment A_1A_2,
F_1 be a middle point of the segment A_3A_4
E_2 be a middle point of the segment A_1A_3
F_2 be a middle point of the segment A_2A_4
E_3 be a middle point of the segment A_1A_4
F_3 be a middle point of the segment A_2A_3

Consider the cross formed by segments $l_1 = E_1F_1, l_2 = E_2F_2, l_3 = E_3F_3$, and consider the subgroup of all permutations of vertices of the tetrahedron, such that the cross remains intact: They will be permuttions $a = (12)(34)$, $b = (13(24)$ and permutation $ab = (14)(23)$. We come to abelian group:

$$KI = \{1, a, b, ab\}$$

It is normal subgroup since it preserves the cross $l_1 l_2 l_3$ in tetraedron $A_1A_2A_3A_4$ Factor-group $S_4 \backslash KI$ acts on the cross. It is group of permutations of edges of CROSS, i.e. it is S_3. We come to

$$S_4 \backslash KI = S_3 \,.$$

Since we know that group S_3 is solvable ($S_3 \backslash C_3 = C_2$), hence S_4 is also solvable. Now perform calculations according our scheme.

Abelian subgroup KI of S_4 has following four characters:

$$\begin{array}{c} \lambda_0 \equiv 1 \\ \lambda_I\colon \quad \lambda_I(1) = 1\,, \lambda_I(a) = 1\,, \lambda_I(b) = -1\,, \lambda_I(ab) = -1 \\ \lambda_{II}\colon \quad \lambda_{II}(1) = 1\,, \lambda_{II}(a) = -1\,, \lambda_{II}(b) = 1\,, \lambda_{II}(ab) = -1 \\ \lambda_{III}\colon \quad \lambda_{III}(1) = 1\,, \lambda_{III}(a) = -1\,, \lambda_{III}(b) = -1\,, \lambda_{III}(ab) = 1 \end{array} \,, \qquad \text{since } a^2 = b^2 = 1.\,,$$

i.e. group of characters of KI is $\hat{KI} = \{\lambda_0, \lambda_I, \lambda_{II}, \lambda_{III}\}$. Respectively for an arbitrary polynomial of roots, $P \in \Sigma^{(4)}$, $P = P(x_1, x_2, x_3, x_4)$ we have

$$P = P_0 + P_I + P_{II} + P_{III} =$$

$$\underbrace{\frac{P + (aP) + (bP) + (abP)}{4}}_{\text{eigenvalues } (1,1,1,1)} + \underbrace{\frac{P + (aP) + (bP) + (abP)}{4}}_{\text{eigenvalues } (1,1,-1,-1)} +$$

$$\underbrace{\frac{P - (aP) + (bP) - (abP)}{4}}_{\text{eigenvalues } (1,1,-1,-1)} + \underbrace{\frac{P - (aP) - (bP) + (abP)}{4}}_{\text{eigenvalues } (1,-1,-1,-1)} +$$

In details:

$(aP)(x_1, x_2, x_3, x_4) = P(x_2, x_1, x_4, x_3)$,
$(bP)(x_1, x_2, x_3, x_4) = P(x_2, x_1, x_4, x_3)$,
$(bP)(x_1, x_2, x_3, x_4) = P(x_3, x_4, x_1, x_2)$,

$$\begin{array}{c} aP_0 = \lambda_0(a)P_0 = P_0\,, bP_0 = \lambda_0(b)P_0\,, abP_0 = \lambda_0(ab)P_0 = P_0 \\ aP_I = \lambda_I(a)P_I = P_I\,, bP_I = \lambda_I(b)P_I = -P_I\,, abP_I = \lambda_I(ab)P_I = -P_I \\ aP_{II} = \lambda_{II}(a)P_{II} = -P_I\,, bP_{II} = \lambda_{II}(b)P_{II} = P_{II}\,, abP_{II} = \lambda_{II}(ab)P_{II} = -P_{II} \\ aP_{III} = \lambda_{III}(a)P_{III} = -P_{III}\,, bP_{III} = \lambda_{III}(b)P_{III} = -P_{III}\,, abP_{III} = \lambda_{III}(ab)P_{III} = P_I \end{array} .$$

Polynomial P_0 is KI-invariant polynomial, all other polynomials are not KI invariants but their squares are. The decomposition of spaces is:

$$\Sigma^{(4)} = \Sigma^{(4)}_{\lambda_0} + \Sigma^{(4)}_{\lambda_I} + \Sigma^{(4)}_{\lambda_{II}} + \Sigma^{(4)}_{\lambda_{III}} \,.$$

The subspace Σ_0 is subspace of $K4$-invariant polynomials.

The square of every polynomial in $\Sigma_I^{(4)}$ or in $\Sigma_{II}^{(4)}$ or in $\Sigma_{III}^{(4)}$ is KI-invariant polynomial. Hence we see that every polynomial can be expressed via KI-invariant polynomials with use of operation of quadratic roots $\sqrt{}$.

On the space of KI-invariant polynomials acts group

$$S_4 \backslash C_3 = S_3$$

i.e. KI invariant polynomials are roots of cubic polynomials.!

Now if we consider polynomial $P = x_1$ we come to the formula for roots of quartic polynomials.

Perform calculations

Suppose that $x_1+x_2+x_3+x_4 = -a$, $x_1x_2+x_1x_3+x_2x_3+\ldots = p$ and $x_1x_2x_3+dots = -q$, $x_1x_2x_3x_4 = r$ i.e. x_1, x_2, x_3 are roots of polynomial $x^4 + ax^3 + p2 + qx + r$. According to decomposition formula we have:

$$x_1 = (x_1)_0 + (x_1)_I + (x_1)_{II} + (x_1)_{III} =$$

$$\underbrace{\frac{x_1+x_2+x_3+x_4}{4}}_{\text{all eigenvalues } 1} + \underbrace{\frac{x_1+x_2-x_3-x_4}{4}}_{\text{eigenvalues } (1,1,-1,-1)} +$$

$$\underbrace{\frac{x_1-x_2+x_3-x_4}{4}}_{\text{eigenvalues } (1,-1,1,-1)} + \underbrace{\frac{x_1-x_2-x_3+x_4}{4}}_{\text{eigenvalues } (1,-1,-1,1)}$$

Denote by

$$u_0 = \frac{x_1+x_2+x_3+x_4}{4}, \quad u_I = \frac{x_1+x_2-x_3-x_4}{4},$$

$$u_{II} = \frac{x_1-x_2+x_3-x_4}{4}, \quad u_{III} = \frac{x_1-x_2-x_3+x_4}{4}.$$

Polynomial w_0 is not only KI-invariant it is S_4-invariant– $u_0 = -a$. Squares of all other polynomials are KI-invarianbt polynomials,i.e. on polynomials $v_I = u_I^2, v_{II} = u_{II}^2, v_{III} = u_{III}^2$ acts the factor group $S_4/KI = S_3$. hence they are roots of cubic polynomial (with coefficeints which are polynomials on $a, p.q.r$).

We see finally that root x_1 is expressed via $u_0, u_I, u_{II}, u_{III}$ via square root operations, and these numbers being roots of cubic equation are expressed via coefficients of polynomials by taking operation of suqre and cube roots. ■