Lueroth theorem; finite group of rational transformations; cubic resolvent, Platonic bodies and Kleinian groups

Notes on reading Shafarevitch e.t.c.

The Lueroth Theorem states the following:

Consider the set of fractions $\{f_1, \dots f_n, \dots\}$ of polynomials with coefficients from some field K. Then there exist a primitive, i.e. a fraction g such that all fractions can be rationally expressed via fraction g. More formally:

Let $K(t)$ be simple transcendent extension of the field K, i.e. field of fractions on indeterminant t. Then every intermediate field is simple extension too. It emans that if L is an intermediate field: $K \subseteq L \subseteq K(t)$ and $L \neq K$ then there exist such $\eta \in K(t)$ that $L = K(\eta)$

Lueroth Theorem is very practical. Consider some examples where application of Lucor Theorem gives a beautiful answer..

Example 1 Let $x = \varphi(t), y = \psi(t)$ be a curve on the plane such that $\varphi(t), \psi(t)$ are rational functions. Then this curve is algebraical curve:

a) there exists a polynomial $P(x, y)$ such that

$$P\left(\varphi(t), \psi(t)\right) \equiv 0$$

and for every point on the curve $P(x, y) = 0$ except finite number of points can be represented as $x = \varphi(t), y = \psi(t)$.

b) in the case if functions $\varphi(t), \psi(t)$ define injection (every point on the curve has a unique parameter) then there exist fraction of polynomials ($R(x, y) = \frac{A(x,y)}{B(x,y)}$) such that

$$t = R(x, y)\big|_{x=\varphi(t), y=\psi(t)}$$

c) In the general case if parametrization $x = \varphi(t), y = \psi(t)$ is not injection one can find another rational parameter $\tau = \tau(t)$ such that new parametrization is already rational injection:

$$\varphi(t) = \tilde{\varphi}(\tau)\big|_{\tau=\tau(t)}, \quad \psi(t) = \tilde{\psi}(\tau)\big|_{\tau=\tau(t)},$$

where $\varphi(\tau), \psi(\tau)$ are fractions and $x = \varphi(\tau), y = \psi(tau)$ is already one-one parametrization.

Let $\varphi(t), \psi(t)$ be fractions of polynomials with *rational coefficients*($\varphi(t), \psi(t) \in \mathbf{Q}(t)$). Then obviously to all rational values of t corresponds the point $x = \varphi(t), y = \psi(t)$ with rational coordinates.

From the previous statement it follows that inverse inclusion is true too:

Every point x, y on the curve $x = \varphi(t), y = \psi(t)$ with rational coordinates has rational parameter (if $\varphi(t), \psi(t) \in \mathbf{Q}(t)$).

E.g. how to describe all points on the circle $x^2 + y^2 = 1$ with rational coordinates (Pythagoras pairs). Circle is defined by rational parametrization via tangent of half-angle: $x = \frac{1-t^2}{1+t^2}, y = \frac{2t}{1+t^2}$ ($x = \cos\theta, y = \sin\theta, t = \tan\frac{\theta}{2}$). (x, y) are rationals if t is rational. Inverse is true. Hence Puthagoras Anzats defines all rational points [1].

Example 2

How to describe the solutions of the equation

$$\frac{f(x)}{g(x)} = \frac{f(t)}{g(t)} \tag{1}$$

Here $\frac{f(t)}{g(t)}$ is a fraction, f, g are coprime polynomials, t parameter. More formally we have to solve the equation (2.1) in the simple transcendent extension of the initial field, or describe extension of the field $K(t)$ generated by the polynomial

$$P_{f/g}(x) = f(x)g(t) - f(t)g(x)\,.P_{f/g} \in K(t)[t] \tag{2}$$

K is arbitrary field. We mostly concetrate on the case when $K = \mathbf{Q}$, or $K = \mathbf{C}$. (Personally I like to think $t = \pi$ (if $K = \mathbf{Q}$)

Suppose that the degree of the fraction $\frac{f(x)}{g(x)}$ is equal to n. Consider an element $\eta = \frac{f(t)}{g(t)}$ in the field $K(t)$ and subfield $\Sigma = K(\eta)$. Then the equation (2.2) can be considered as polynomial over field Σ. Equation (2.2) obviously has one root $x = t$ in $K(t)$. Polynomial $f(x) - \eta g(x)$ (polynomial over Σ) is irreducible. (This follows from Gauss lemma and from the fact that polynomial (2.1) is irreducible in the *ring* of plynomials) Hence $K(t)$ is extension of $K(\eta)$ of degree N.

Now we pose very beautiful question. Other roots of equation (2.1) belong to $K(t)$ or not. Or in the other words

$$\textit{is extension } K(t) : K(\eta) \textit{ an algebraic extension?} \tag{4}$$

or equivalently

does the equation (2.1) possess all N roots in the field $K(t)$

Reflecting on Lueroth Theorem and answering this question I realized that I invented the wheel finally understanding what about is Klein book (which I loosed...)

[1] When I was in school I liked to stress the fact that it is very important that not only the Anzats $x = \frac{1-t^2}{1+t^2}, x = \frac{1-t^2}{1+t^2}$ is rational but inverse $t = \frac{y}{1-x}$ is rational too. The Lueroth Theorem explains it.

Suppose that the fraction f/g possesses N symmetries! Then obviously equation (2.1) possesses N roots. (E.g. fraction $x-1/x$) posesses 2 symmetries ($x \to -1/x$). Respectively the the equation $\frac{x^2-1}{x} = \frac{t^2-1}{t}$ has roots $x_1 = t, x_2 = -\frac{1}{t}$)

Study the inverse. Suppose the equation (2.1) has N roots in $K(t)$. According Galois considerations there are N automorphisms of $K(t)$ which are fixed on $K(\eta)$. Every Galois automorphism of $K(t)$ it is fractional-linear transformation $t \to \frac{at+b}{ct+d}$. We come to N rational transformations preserving the fraction f/g.

If finite group G acts on $K(t)$ then the fraction

$$\sum_{g \in g} t^g$$

is a fraction which possesses G-symmetries.

Omitting important but boring considerations I will go to very beautiful example:

Consider the action of the cyclic group G_3 containing $N = 3$ elements on the complex plane:

$$\sigma\colon t \to -\frac{1}{1+t}, \quad \sigma^2\colon\ t \to -1 - \frac{1}{t}, \sigma^3 = \mathbf{id}$$

Consider polynomial with three roots $z = t, z = -\frac{1}{1+t}, z = -1 - \frac{1}{t}$

$$P(z) = (z-t)\left(z + \frac{1}{1+t}\right)\left(z + 1 + \frac{1}{t}\right)$$

On the other hand consider G_3-invariant fraction (later we will call it just G-fraction)

$$F_G(t) = f(t)/g(t) = t + \sigma(t) + \sigma^2(t) = t - \frac{1}{1+t} - 1 - \frac{1}{t} = \frac{t^3 - 3t - 1}{t(t+1)}$$

It i evident that equation

$$F_G(z) = F_G(t), \quad \text{i.e.} \quad \frac{z^3 - 3z - 1}{z(z+1)} = \frac{t^3 - 3t - 1}{t(t+1)}$$

has the same roots. Hence polynomial $P(z)$ is proportional to $f(z)g(t) - f(t)g(z)$.

Note also that numerator is resolvent cubic...

What happened. In fact for a given group Γ we constructed normal extension such that G is Galois group of this extension in the case if G is discrete subgroup of $GL(2, \mathbf{C})$. Indeed let

$$\Gamma = \{g_1, \ldots, g_N\}$$

Let K be extension of Q by coefficients of $\{g_i\}$ and $K(t)$ be transcendent extension of K (in other words t is a parameter) Then polynomial

$$P_G(z) = \prod_{i=1}^{N}(z - t^{g_i})$$

is polynomial over the subfield $K(\eta)$ where Γ-fraction η can be defined as non-trivial symmetrization of t under the action of group Γ (e.g. $t = \sum_i t^{g_i}$ if it is not equal to zero)

More serious considerations (invariance groups of Platonic bodies is just the content of Klein's book)

§2 **Action of** G_N

Inventing the wheel I considered fraction which is invariant under cyclic finite subgroup G_3 of $SL(2, \mathbf{Z})$. (see above) and came to the fraction $\frac{x^3-3x-1}{x^2+x}$. On the other hand the numerator of this fraction famous irreducible cubic with all Galois group is just G_3.

The simplest way to find the fraction invariant under G_3 it is to consider $F = z^3$. Here we will make the from $F = x^3$ to $F = \frac{x^3-3x-1}{x^2+x}$. Making this bridge we see how important are ramification points. We will try to understand the relation with roots $2\cos\frac{\pi}{9}, ...$ of the famous cubic.

Consider the function

$$F_N = z^N \tag{2.1}$$

This function defines N-covering $C \to C$ with two ramification points $0, \infty$. Transformation

$$z \to ze^{i\varphi}, \varphi = \frac{2\pi}{N} \tag{2.2}$$

is generator of symmetry transformations.

Rational transformation $z \to \frac{az+b}{cz+d}$ transforms points $[0, \infty]$ to $[b/d, a/c]$.

One can consider the transformation

$$w = w(z) = \frac{z + \varepsilon}{z/\sigma + 1}, \tag{2.3}$$

with inverse

$$z = \frac{w - \varepsilon}{1 - w/\sigma} \tag{2.3a}$$

Then $[0, \infty] \to [\varepsilon, \sigma]$.

The generator of symmetry transformations for $w \to \tilde{w} = h(w)$ will be

$$w \to w\left[z\left(w\right)e^{i\varphi}\right] = \frac{\left[\frac{w-\varepsilon}{1-w/\sigma}e^{i\varphi}\right] + \varepsilon}{\left[\frac{w-\varepsilon}{1-w/\sigma}\frac{e^{i\varphi}}{\sigma}\right] + 1} =$$

$$\frac{\sigma(w-\varepsilon)e^{i\varphi}+(\sigma-w)\varepsilon}{(w-\varepsilon)e^{i\varphi}+(\sigma-w)}=\frac{w(\sigma e^{i\varphi}-\varepsilon)-\sigma\varepsilon(e^{i\varphi}-1)}{w(e^{i\varphi}-1)+(\sigma-\varepsilon e^{i\varphi})} \tag{2.4}$$

The points $[\varepsilon,\sigma]$ will be ramification point for the function:

$$\tilde{F}(w)=\left(z\left(w\right)\right)^N=\left(\frac{w-\varepsilon}{1-w/\sigma}\right)^N \tag{2.5}$$

This function remains invariant under symmetry transformations (2.5).

Every rational fraction which is invariant under the symmetry transformations (2.5) is rational fraction on (2.5). (It is nothing but Lueroth Theorem, because set of all G-ivariant functions is subfield). E.g.the function:

$$\frac{f(w)}{g(w)}=w+h(w)+h(h(w))+\ldots$$

must be rational function on (2.5).

Is it right that every rational function which gives N-covering with ramification points $[\varepsilon,\sigma]$ is **rational function of the function (2.4)**? (*je crois que c'est vraie*)

Symmetry transformations $w\to w$ (2.4) do not move ramification points $[\varepsilon,\sigma]$ of the function (2.5) and arbitrary rational function of (2.5) and do not move values of these functions, as well as symmetry transformations $z\to ze^{i\varphi}$ do not move ramification points $[0,\infty]$ of the function z^N and arbitrary rational function of z^N and do not move the values of these functions.

Consider (for formulae look more readable) the case when ramification points are the following N-roots of unity:

$$\varepsilon=e^{i\varphi},\sigma=e^{-i\varphi} \tag{2.6}$$

As before we suppose $e^{i\varphi}=e^{\frac{2i\pi}{N}}$. (It has sense if $N\geq 3$)

Then symmetry transformations (2.5) look very nice:

$$w\to\frac{w(\sigma e^{i\varphi}-\varepsilon)-\sigma\varepsilon(e^{i\varphi}-1)}{w(e^{i\varphi}-1)+(\sigma-\varepsilon e^{i\varphi})}=\frac{w(1-e^{i\varphi})-(e^{i\varphi}-1)}{w(e^{i\varphi}-1)+(e^{-i\varphi}-e^{2i\varphi})}= \tag{2.7}$$

$$\frac{(w+1)\sin\frac{\varphi}{2}}{\sin\frac{3\varphi}{2}-w\sin\frac{\varphi}{2}}=\frac{w+1}{\sin\frac{3\varphi}{2}/\sin\frac{\varphi}{2}-w}$$

(Where from number 3 appears?)

What is it the meaning of the last formula?

For arbitrary cyclic group G_N we calculated symmetry transformation of rational fractions with rational coefficients plus the number

$$\delta_N=\frac{\sin\frac{3\varphi}{2}}{\sin\frac{\varphi}{2}}=\frac{\sin\frac{3\pi}{N}}{\sin\frac{2\pi}{N}} \tag{2.8}$$

In other way we did in this section the following:

Let $K_N = \mathbf{Q}(\delta_N)$ be an extension of rationales by algebraic number δ_N defined by (2.8).

The group of all transformations $t \to \frac{at+b}{ct+d}$ (with coefficients depended on δ_N) is the Galois group of transcendent field extension $K(t) : K$.

The subfield of $K(t)$ which is invariant under the transformation of group G_N (its action on $K(t)$ is generated by (2.6)). We have to consider G-invariant function. It can be (2.5) or averaging of w by the action (2.7) of group.

The field $K_N(t)$ is Galois extension over the field $K_N(\eta)$ where η is G-invariant fraction... Better consider examples.

§3 Example for G_3 and relation with polynomial $x^3 - 3x - 1$

1. $N = 3$. The transformation (2.7) is $w \to w + 1w = -1 - \frac{1}{w}$ generates cyclic group action with three elements. G_3-invariant function e.g.

$$w + \left(-1 - \frac{1}{w}\right) + \left(\frac{-1}{w+1}\right) = \frac{w^3 - 3w - 1}{w(w+1)} \tag{3.1}$$

can be considered as primitives. Arbitrary G_3 function which has degree 3 and ramification points $[e^{\frac{2i\pi}{3}}, e^{\frac{-2i\pi}{3}}]$ has to be rational function of $\eta = \frac{w^3-3w-1}{w(w+1)}$*

In this example mysteriously arises famous cubic resolvent. Why?

Try to come to the fraction (3.1) in a little bit different way.

Instead coordinate w consider homogeneous coordinates $[x : y]$. $\frac{w=x}{y}$.

The action of transformation (2.7) is in terms of (x, y):

$$\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ -x \end{pmatrix} \tag{3.2}$$

Eigen-forms of this linear transformation are

$$F_1 = \lambda x + y, F_2 = x + \lambda y, \quad \text{where} \quad \lambda = e^{\frac{i\varphi}{2}}:$$

$$\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} x+y \\ -x \end{pmatrix} \qquad \begin{pmatrix} F_1 \\ F_2 \end{pmatrix} \to \begin{pmatrix} e^{\frac{i\varphi}{2}} F_1 \\ e^{\frac{-i\varphi}{2}} F_2 \end{pmatrix} \tag{3.3}$$

zv It is easy to see that relative invariants of degree 3 are

$$\{sF_1^3 + tF_2^3, F_1^2 F_2, F_1 F_2^2\}$$

* Je crois que more: every one-one function analytical on extended complex plane is linear fraction. Hence condition of rationality and invariance can be weakened.... Comment?

Absolute invariants in particlularly:

$$\frac{sF_1^3+tF_2^3}{s'F_1^3+t'F_2^3} \tag{3.4}$$

E.g. the cubic

$$sF_1^3+tF_2^3=0 \tag{3.5}$$

has Galois group G_3. On the other hand roots of this cubic can be calculated directly: (We come to linear equation: $s^{1/3}(x+\lambda y)+t^{1/3}(y+\lambda x)=0$) Study the properties of this equation. (Do not forget that our considerations here are mimicking Klein...)

First of all note that by construction the Galois group of the cubic equations over field of coefficients is cyclic (if cubic is irreducible).The point is that field of coefficients contains irrationality. (It is just what happened when we add $\sqrt{D}$ to the field)

Now return to cubic x^3-3x-1. Its Galois group is G_3 because discriminant is rational (and cubic irreducible) Galois transformations acing on roots are

$$x\to 2-x^2$$

and it is same as

$$x\to -1-\frac{1}{x} \tag{3.6}$$

The same are properties of (3.5). Write down in details (3....):

$$sF_1+tF_2=s(x+\lambda y)^3+t(y+\lambda y=x)^3=$$

$$(s-t)(x^3-y^3)+3(s\lambda+t\lambda^2)x^2y+3(t\lambda+s\lambda^2)y^2x, \qquad (\lambda=e^{\frac{i\varphi}{2}}=e^{\frac{i\pi}{3}}) \tag{3.7}$$

$\lambda^2-\lambda+1=0$ Denote by

$$\kappa=\frac{s\lambda+t\lambda^2}{s-t}$$

Then $t\lambda+s\lambda^2=(s-t)(\kappa-1)$ and

$$sF_1+tF_2=(s-t)\left(x^3-y^3+3\kappa x^2y-3(1-\kappa)xy^2\right)$$

In particular If $\kappa=0,1$ then we come to glorious cubic. (If $k=1$ then transformation $x\to x-1$ is rational) In general case we have cubic:

$$x^3+3\kappa x^2-3(1-\kappa)x-1=0, \kappa=se^{\frac{2i\pi}{3}}+te^{\frac{i\pi}{3}} \tag{3.8}$$

Of course in general case considering $x\to x-\kappa/3$ we come to reduced cubic x^3

$$x^3-p(k)x-q(k) \tag{3.9}$$

This cubic is generic. Why Galois group is G_3, not S_3. The reason is that here Galois group transformations are over field $Q(\delta)$. In some sense the last equation gives as another? algorithm to solve cubic: reduce cubic to the form (3.9) then (3.8). The equation (3.8) has solution: From $sF_1^3 + tF_2^3 = 0$ we come to

$$s^{1/3}(x + \lambda y) + t^{1/3}(y + \lambda x) = 0$$

Hence the root

$$\theta = \frac{x}{y} = -\frac{\sqrt[3]{t} + \lambda\sqrt[3]{s}}{\sqrt[3]{s} + \lambda\sqrt[3]{t}}$$

and other roots are defined by Galois group:

$$\theta_2 = -1 - \frac{1}{\theta}, \theta_3 = -\frac{1}{\theta + 1}$$

In particular if $\kappa(s - t) = s\lambda + t\lambda^2 = 0$, i.e. $s = \lambda^2, t = -\lambda$ then

$$\theta = \frac{\lambda^{\frac{1}{3}} - \lambda^{\frac{5}{3}}}{\lambda^{\frac{2}{3}} - \lambda^{\frac{4}{3}}} = \lambda^{-\frac{1}{3}} + \lambda^{\frac{1}{3}} = 2\cos\frac{\pi}{9}$$

All that is done here is just two words in Klein book5. But I already understand them.

Kleinian groups

My reflections on Lueroth Theorem lead me to the question about so called nice fractions,i.e. fractions such that equation $F(x) = F(t)$ have N rational solutions (including $x = N$). Thus we come to discrete group acting on plane. Thus we come to the famous Klein group where in particular I found the proof of the fact that finite groups corresponding to Platon bodies, it is all! What really is curious that the proof is similar? to the proof about existence of Platonic bodies. Like in that case we have to solve Diophantian equation:

$$\sum \frac{N}{\nu_i}(\mu_i - 1) = 2N - 2$$

Remember that in the case of Platonic bodies we solve equation:

$$\frac{2E}{\nu} - E + \frac{2E}{n} = 2$$

In the first case N is the number of elements of discrete group, ν_i index of roots. In the second case E is number of edges of Platonic body,ν number of edges at the give vertex,n

5 In fact I study here the case of cyclic group (even not diedre) with ramification points not at $[0, \infty]$ From the general pont of view this makes situation less clear.

number of sides of every side. The fact that we consider sphere is evidently used in the second. How it is used in first? (Or may be here where sphere is simplest... we do not need specify??)

Hovik Khudaverdian 2 VII 2004
Manchester