

Cubic and quadric equations; Galois theory for pedestrians.

*This text is written on the base of the book of A. Khovansky "Galois Theory"*

We suppose that Galois group exists. This is not trivial....

We suppose that the main field is a field of characteristic 0 which possesses all roots of unity.

In this lecture the expression "can be expressed" means.....

Begin with Vieta Theorem. It tells that

Consider polynomial

$$P(t) = x^n + \dots$$

Then roots of this polynomial obey relations

Let  $\Sigma(x_1, \dots, x_n)$  be polynomial on variables  $x_1, \dots, x_n$ . This polynomial can be expressed via co

**Proposition 1** Let  $A$  be an algebra over field  $K$ , and let  $H$  be a finite abelian group acting on algebra  $A$ . Denote by  $A_H$  elements of algebra  $A$  which are invariant under the action of group  $H$ .

Then an arbitrary element of algebra  $A$  can be expressed via elements of invariant subalgebra  $A_H$  by taking roots.

Example.

1) Quadratic equation. Algebra  $A$  is generated by roots of polynomial Abelian group  $H = (1, \sigma)$ .  $\sigma(x_1, x_2) = (x_2, x_1)$ .

Consider  $u = x_1 + x_2$ ,  $t = (x_1 - x_2)^2$ . These elements are  $H$ -invariant.  $\frac{x_1 - x_2}{2} = \frac{u + \sqrt{t}}{2}$

**Theorem** Let  $G$  be a group and  $H$  be its invariant subgroup, such that group  $H$  and group  $G/H$  are abelian groups.

$$1 \triangle H \triangle G$$

Then every element of algebra  $A$  can be expressed via  $G$ -invariants of algebra  $A$  by taking operations of roots.

Indeed group  $H$  acts on algebra  $A$ , and abelian group  $G/H$  acts on  $H$ -invariants of algebra  $G$ . Hence by Proposition 1, an arbitrary element  $x \in A$  can be expressed via  $H$ -invariants of algebra  $A$ . On the other hand since abelian group  $G/H$  acts on  $H$ -invariants, every  $H$ -invariant in its turn can be expressed via  $G/H$  invariants, i.e.  $G$ -invariants of algebra  $A$ .

Denote by  $A_G$  the set of elements of the algebra  $A$  which are invariant

Then every element  $x$  of the algebra  $A$  can be represented as a sum of elements  $w_1, \dots, w_k$  such that every  $w$

Then there exists basis

We will use the following lemma:

Let  $L$  be linear operator on finite-dimensional vector space  $V$  over field which possesses roots of unity. Then  $L$  is diagonalisable. Proof see in Appendix 1.

Calculations for cubic equation

Consider the cubic equation

$$x^3 + ax^2 + px + q = 0$$

where coefficients are complex numbers. We will put  $a = 0$  almost for all calculations, but sometimes it will be useful to consider  $a$  as an arbitrary complex number.

We have

$$\begin{aligned} x_1 + x_2 + x_3 &= -a \\ x_1x_2 + x_2x_3 + x_3x_1 &= p \\ x_1x_2x_3 &= -q \end{aligned}$$

Take root  $x_1$ . Consider linear space spanned by the orbit of the element  $x_1$  under the action of the cyclic group  $C_3$ :

$$C_3 = \{1, s, s^2\}, \quad s = (123), s^2 = (132).$$

We have  $sx_1 = x_2, sx_2 = x_3$ . The linear space  $V_1$  is space spanned by vectors  $\{x_1, sx_1, s^2x_1\}$ . Its dimension is  $\leq 3$ .

The group  $C_3$  is commutative group. Find a basis  $(w_1, w_2, w_3)$  of eigenvectors [‘states’ which are simultaneously measurable]

$$sw_1 = \delta_1 w_1 \quad sw_2 = \delta_2 w_2 \quad sw_3 = \delta_3 w_3, .$$

One can see that this is so called Lagrange variables

$$\begin{aligned} w_0 &= x_1 + x_2 + x_3, & sw_0 &= w_0 \\ w_1 &= x_1 + \varepsilon^2 x_2 + \varepsilon x_3, & sw_1 &= \varepsilon w_1 \\ w_2 &= x_1 + \varepsilon x_2 + \varepsilon^2 x_3, & sw_2 &= \varepsilon^2 w_2 \end{aligned}$$

One can see that

$$x = \frac{w_0 + w_1 + w_2}{3}.$$

We calculate  $w_0, w_1, w_2$ .  $w_0 = a$  is a coefficient.

Later during detailed calculations we put  $w_0 = a = 0$ .

Consider numbers

$$z = w_1^3 + w_2^3, t = (w_1^3 - w_2^3)^2$$

These numbers are invariants of all permutations, i.e. they are polynomials of coefficients. Calculate these numbers (assuming  $w_0 = x_1 + x_2 + x_3 = 0$ ):

We will use the following identity:

$$a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - ab - ac - bc). \quad (8)$$

$$\begin{aligned}
z &= (x_1 + \varepsilon^2 x_2 + \varepsilon x_3)^3 + (x_1 + \varepsilon x_2 + \varepsilon^2 x_3)^3 = 2(x_1^3 + x_2^3 + x_3^3) + 12x_1x_2x_3 + \\
&3x_1x_2\varepsilon(x_1 + x_2)(1 + \varepsilon) + 3x_2x_3\varepsilon(x_2 + x_3)(1 + \varepsilon) + 3x_3x_1\varepsilon(x_3 + x_1)(1 + \varepsilon) = \\
&\text{(with use of identity (*))}
\end{aligned}$$

$$6x_1x_2x_3 + 12x_1x_2x_3 - 9\varepsilon(1 + \varepsilon)x_1x_2x_3 = 27x_1x_2x_3 = -27q.$$

It is little bit more long to calculate  $t$

$$\begin{aligned}
t &= [(x_1 + \varepsilon^2 x_2 + \varepsilon x_3)^3 - (x_1 + \varepsilon x_2 + \varepsilon^2 x_3)^3]^2 = \\
&[3x_1x_2\varepsilon(x_1 - x_2)(\varepsilon - 1) + 3x_2x_3\varepsilon(x_2 - x_3)(\varepsilon - 1) + 3x_3x_1\varepsilon(x_3 - x_1)(\varepsilon - 1)]^2 = \\
&(3\varepsilon(\varepsilon - 1))^2 [x_1x_2(x_1 - x_2) + x_2x_3(x_2 - x_3) + x_3x_1(x_3 - x_1)]^2 = \\
&-27 [x_1^2x_2^2(x_1 - x_2)^2 + x_2^2x_3^2(x_2 - x_3)^2 + x_3^2x_1^2(x_3 - x_1)^2] - \\
&-27 [2x_1^2x_2x_3(x_1 - x_2)(x_3 - x_1) + 2x_2^2x_3x_1(x_1 - x_2)(x_2 - x_3) + 2x_3^2x_1x_3(x_2 - x_3)(x_3 - x_1)] = \blacksquare \\
&-27 [x_1^2x_2^2(x_1 + x_2)^2 + x_2^2x_3^2(x_2 + x_3)^2 + x_3^2x_1^2(x_3 + x_1)^2 - 4(x_1^3x_2^3 + x_1^3x_3^3 + x_2^3x_3^3)] - \\
&-54x_1x_2x_3 [x_1(-x_1^2 - x_2x_3 + x_1(x_2 + x_3)) + x_2(-x_2^2 - x_1x_3 + x_2(x_1 + x_3)) + x_3(-x_3^2 - x_1x_2 + x_3(x_1 + x_2))]
\end{aligned}$$

Now again using the identity (\*) we come to

$$\begin{aligned}
&-27 \left[ 3x_1^2x_2^2x_3^2 - 4 \left( \underbrace{x_1^3x_2^3 + x_1^3x_3^3 + x_2^3x_3^3}_K \right) \right] - 54x_1x_2x_3 [-2(x_1^3 + x_2^3 + x_3^3) - 3x_1x_2x_3] = \\
&-72x_1^2x_2^2x_3^2 - 54x_1x_2x_3 [-6x_1x_2x_3 - 3x_1x_2x_3] + 108K = 27 [27x_1^2x_2^2x_3^3 + 4(x_1x_2 + x_2x_3 + x_3x_1)^3] = \blacksquare \\
&27(27q^2 + 4p^3).
\end{aligned}$$

since due to identity (\*)

$$\begin{aligned}
K &= x_1^3x_2^3 + x_1^3x_3^3 + x_2^3x_3^3 = 3x_1^2x_2^2x_3^2 + (x_1x_2 + x_1x_3 + x_2x_3) [(x_1x_2 + x_1x_3 + x_2x_3)^2 - 3x_1x_2x_3(x_1 + x_2 + x_3)] \\
&= 3x_1^2x_2^2x_3^2 + (x_1x_2 + x_1x_3 + x_2x_3)^3.
\end{aligned}$$

Finally we have

$$\begin{aligned}
&\begin{cases} z = w_1^3 + w_2^3 = -27q \\ t = (w_1^3 - w_2^3)^2 = 27^2 \left( q^2 + \frac{4p^3}{27} \right) \end{cases}, \text{ i.e. } w_1^3, w_2^3 = 27 \left( -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \right) \\
x_1 &= \frac{1}{3} \frac{w_0 + w_1 + w_2}{3} = \frac{1}{3} (\sqrt[3]{w_1} + \sqrt[3]{w_2}) = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \quad (\dagger)
\end{aligned}$$

**Remark** A question remains: what branch of cubic root has to be taken?

Answer: Consider  $R = w_1 w_2$ . This magnitude is invariant with respect to all permutations since

$$s w_1 = \varepsilon w + 1, s w_2 = \varepsilon^2 w_2 \quad \text{and} \quad \sigma_{12} w_1 = w_2$$

Hence it is a symmetric polynomial on roots, i.e. polynomial on coefficients. Calculate the answer:

$$w_1 w_2 = (x_1 + \varepsilon^2 x_2 + \varepsilon x_3)(x_1 + \varepsilon x_2 + \varepsilon^2 x_3) = (x_1^2 + x_2^2 + x_3^2) + (x_1 x_2 + x_1 x_3 + x_2 x_3)(\varepsilon + \varepsilon^2) =$$

$$(x_1^2 + x_2^2 + x_3^2) - (x_1 x_2 + x_1 x_3 + x_2 x_3) = (x_1 + x_2 + x_3)^2 - 3(x_1 x_2 + x_1 x_3 + x_2 x_3)^2 = a^2 - 3p^2. \quad \dagger$$

Changing  $w_1 \mapsto \varepsilon w_1$ ,  $w_2 \mapsto \varepsilon^2 w_2$  is Galois symmetry. This condition fixes the branches. E.g. in the case  $a = 0$  we have to choose the branches such that

$$w_1 w_2 = \sqrt[3]{27 \left( -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \right)} \sqrt[3]{27 \left( -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \right)} = -3p^2.$$

In particular if  $\left( \frac{q^2}{4} + \frac{p^3}{27} \right) > 0$ , then one considers the branch that takes real values on real numbers, then  $x_1$  in equation \*\* becomes real root, and

$$x_2 = \varepsilon \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \varepsilon^2 \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \quad x_3 = \varepsilon^2 \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \varepsilon \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \quad (\dagger\dagger)$$

are two complex roots. E.g. for equation  $x^2 + 3x - 18$  we have three roots:

$$\begin{cases} x_1 = \sqrt[3]{-9 + \sqrt{80}} + \sqrt[3]{9 - \sqrt{80}} = 3 \\ x_2 = \varepsilon \sqrt[3]{9 + \sqrt{80}} + \varepsilon^2 \sqrt[3]{9 - \sqrt{80}} \\ x_3 = \varepsilon \sqrt[3]{9 + \sqrt{80}} + \varepsilon^2 \sqrt[3]{9 - \sqrt{80}} \end{cases} \quad \left( \varepsilon = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \right).$$

To see that problem of choosing branch can be non-trivial consider the following ‘non-clever solution’ of the cubic equation:

Non-clever solution

Solve again the equation  $x^3 + px + q = 0$  with

$$\begin{aligned} x_1 + x_2 + x_3 &= 0 \\ x_1 x_2 + x_2 x_3 + x_3 x_1 &= p \\ x_1 x_2 x_3 &= -q \end{aligned}$$

but now we introduce Lagrange variables in not clever way:

$$\begin{aligned} w_0 &= x_1 + x_2 + x_3 \\ w_I &= x_1 + \varepsilon x_2 + \varepsilon^2 x_3 \\ w_{II} &= x_2 + \varepsilon x_1 + \varepsilon^2 x_3 \end{aligned} \quad \left( \varepsilon = e^{\frac{2\pi i}{3}} \right).$$

(Compare how we have chosen  $w_1, w_2$  before)

$$w_0 = 0.$$

Still we calculate in the same way:

$$\begin{aligned} w_0^3 &= 0 \\ u = w_I^3 &= x_1^3 + x_2^3 + x_3^3 + 3\varepsilon(x_1^2x_2 + x_2^2x_3 + x_3^2x_1) + 3\varepsilon^2(x_1x_2^2 + x_2x_3^2 + x_3x_1^2) + 6x_1x_2x_3 \\ v = w_{II}^3 &= x_1^3 + x_2^3 + x_3^3 + 3\varepsilon^2(x_1^2x_2 + x_2^2x_3 + x_3^2x_1) + 3\varepsilon(x_1x_2^2 + x_2x_3^2 + x_3x_1^2) + 6x_1x_2x_3 \end{aligned}$$

Hence

$$u + v = 2(x_1^3 + x_2^3 + x_3^3) + 3\varepsilon(1 + \varepsilon)(x_1^2x_2 + \dots) + 12x_1x_2x_3$$

... means all permutations. Since

$$a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - ab - ac - bc), \quad (*)$$

$w_0 = 0$  and  $\varepsilon(1 + \varepsilon) = -1$ , hence

$$u + v = 6x_1x_2x_3 - 3(x_1x_2(-x_3) + x_1x_3(-x_2) + x_2x_3(-x_1)) + 12x_1x_2x_3 = 27x_1x_2x_3 = -27q, \blacksquare$$

$$\begin{aligned} u - v &= 3(\varepsilon - \varepsilon^2)(x_1^2x_2 + x_2^2x_3 + x_3^2x_1) + 3(\varepsilon^2 - \varepsilon)(x_1x_2^2 + x_2x_3^2 + x_3x_1^2) = \\ &= 3(\varepsilon - \varepsilon)^2(x_1x_2(x_1 - x_2) + x_2x_3(x_2 - x_3) + x_3x_1(x_3 - x_1)) \end{aligned}$$

and

$$(u - v)^2 = 9(\varepsilon - \varepsilon^2)^2 [x_1x_2(x_1 - x_2) + x_2x_3(x_2 - x_3) + x_3x_1(x_3 - x_1)]^2 = -27[K + L],$$

where

$$K = x_1^2x_2^2(x_1 - x_2)^2 + x_2^2x_3^2(x_2 - x_3)^2 + x_3^2x_1^2(x_3 - x_1)^2,$$

$$L = 2x_1x_2x_3 [x_1(x_1 - x_2)(x_3 - x_1) + x_2(x_1 - x_2)(x_2 - x_3) + x_3(x_2 - x_3)(x_3 - x_1)].$$

using equation (\*) and fact that  $x_1 + x_2 + x_3 = 0$  we see that

$$\begin{aligned} K &= x_1^2x_2^2(x_1 + x_2)^2 + x_2^2x_3^2(x_2 + x_3)^2 + x_3^2x_1^2(x_3 + x_1)^2 - 4(x_1^3x_2^3 + x_2^3x_3^3 + x_3^3x_1^3) =, \\ &= 3x_1^2x_2^2x_3^2 - 4(x_1x_2 + x_2x_3 + x_3x_1)(x_1^2x_2^2 + x_2^2x_3^2 + x_3^2x_1^2 - x_1^2x_2x_3 - x_1x_2^2x_3 - x_1x_2x_3^2) - 12x_1^2x_2^2x_3^2 \\ &= -9x_1^2x_2^2x_3^2 - 4(x_1x_2 + x_2x_3 + x_3x_1) [(x_1x_2 + x_2x_3 + x_3x_1)^2 - 3(x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2)] = \blacksquare \\ &= -9x_1^2x_2^2x_3^2 - 4(x_1x_2 + x_2x_3 + x_3x_1)^3 = -9q^2 - 4p^3. \end{aligned}$$

and

$$L = 2x_1x_2x_3 [x_1(x_1 - x_2)(x_3 - x_1) + x_2(x_1 - x_2)(x_2 - x_3) + x_3(x_2 - x_3)(x_3 - x_1)] = 2x_1x_2x_3M. \blacksquare$$

with

$$\begin{aligned}
M &= x_1(x_1 - x_2)(x_3 - x_1) + x_2(x_1 - x_2)(x_2 - x_3) + x_3(x_2 - x_3)(x_3 - x_1) = \\
&(-x_1^3 + x_1(x_2 + x_3) - x_1x_2x_3) + (-x_2^3 + x_2(x_1 + x_3) - x_1x_2x_3) + (-x_3^3 + x_3(x_1 + x_2) - x_1x_2x_3) = \\
&-2(x_1^3 + x_2^3 + x_3^3) - 3x_1x_2x_3 = -9x_1x_2x_3
\end{aligned}$$

since  $x_1 + x_2 + x_3 = 0$ . Hence

$$L = 2x_1x_2x_3M = -18x_1^2x_2^2x_3^2 = -18q^2.$$

We come to

$$(u - v)^2 = -27(K + L) = -27(-9q^2 - 4p^3 - 18q^2) = 27(27q^2 + 4p^3).$$

Finally we have

$$\begin{cases} u + v = w_I^3 + w_{II}^3 = -27q \\ u - v = w_I^3 - w_{II}^3 = \pm 27\sqrt{q^2 + \frac{4p^3}{27}} \end{cases}$$

or:

$$\begin{cases} w_0 = x_1 + x_2 + x_3 \\ w_I = x_1 + \varepsilon x_2 + \varepsilon^2 x_3 \\ w_{II} = x_2 + \varepsilon x_1 + \varepsilon^2 x_3 \end{cases} \quad (\varepsilon = e^{\frac{2\pi i}{3}}), \quad \text{with} \quad \begin{cases} w_I^3 + w_{II}^3 = -27q \\ w_I^3 - w_{II}^3 = \pm 27\sqrt{q^2 + \frac{4p^3}{27}} \end{cases}$$

One can easily solve the system of linear equations using the fact that  $1 + \varepsilon + \varepsilon^2 = 0$ . E.g. adding first equation multiplied by  $\varepsilon^2$  with second and third we come to the answer for  $x_3$  and so on:

$$\begin{cases} x_1 = \frac{w_I + \varepsilon^2 w_{II}}{3} \\ x_2 = \frac{w_{II} + \varepsilon^2 w_I}{3} \\ x_3 = \frac{(w_I + w_{II})\varepsilon}{3} \end{cases}, \quad \text{with} \quad \begin{cases} w_I^3 + w_{II}^3 = -27q \\ w_I^3 - w_{II}^3 = \pm 27\sqrt{q^2 + \frac{4p^3}{27}} \end{cases}$$

i.e.

$$\begin{cases} w_I^3 = 27\left(-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\right) \\ w_{II}^3 = 27\left(-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\right) \end{cases} \quad \text{or} \quad \begin{cases} w_I^3 = 27\left(-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\right) \\ w_{II}^3 = 27\left(-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\right) \end{cases}$$

(We suppose that the branch of function  $\sqrt{\phantom{x}}$  is chosen) These equations define  $w_I, w_{II}$  not uniquely. There are man solutions:

$$\begin{aligned}
w_I &= 3 \left( -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \right), w_{II} = 3 \left( -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \right) \\
w_I &= 3\varepsilon \left( -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \right), w_{II} = 3 \left( -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \right) \\
w_I &= 3 \left( -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \right), w_{II} = 3 \left( -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \right) \\
w_I &= 3 \left( -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \right), w_{II} = 3 \left( -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \right) \\
w_I &= 3 \left( -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \right), w_{II} = 3 \left( -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \right) \\
w_I &= 3 \left( -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \right), w_{II} = 3 \left( -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \right)
\end{aligned}$$

**Remark** These are solutions of sixth order resolvent equations. On the other hand we need solutions of cubic equation. How?

Return again to invariant

$$R = w_I w_{II}$$

This is invariant of all permutations. Calculate it:

$$w_I w_{II} = (x_1 + \varepsilon x_2 + \varepsilon^2 x_3)(\varepsilon x_1 + x_2 + \varepsilon^2 x_3) = (1 + \varepsilon^2)(x_1 x_3 + x_1 x_2 + x_2 x_3) + \varepsilon(x_1^2 + x_2^2 + x_3^2) =$$

$$\varepsilon(x_1 + x_2 + x_3)^2 + (\varepsilon^2 + 1 - 2\varepsilon)(x_1 x_3 + x_1 x_2 + x_2 x_3) = \varepsilon(x_1 + x_2 + x_3)^2 - 3\varepsilon(x_1 x_3 + x_1 x_2 + x_2 x_3) = a\varepsilon - 3p^3\varepsilon \blacksquare$$

(Compare with previous answer (†)) Here we see that we have to take such branches tht the condition above holds. E.g. in the case of one real root we have to multiply on  $\varepsilon^2$ .

## Appendix

Let  $L^N = 1$ .

We have to prove that operator  $L$  does not possess no-trivial Jorda cells. Suppose it possesses non-trivial Jorda cell, i., there is a subspace  $V$  such that  $L$  on this subspace is an operator  $L = \lambda + I$ , where  $I$  is nilpotent operator, and  $\lambda = e^{\frac{2\pi i s}{N}}$  is a root of unity. We have that  $I^m = 0$ , where  $m$  is a size of Jordan cell, we have to prove that  $m = 1$ ,  $I = 0$ . Take an arbitrary vector  $\mathbf{x}$ . Prove that  $I\mathbf{x} = 0$ . If this is not the case then there exists  $k$ , ( $2 \leq k \leq m$ ) such that  $I^k \mathbf{x} = 0$ , but  $I^{k-1} \mathbf{x} \neq 0$ , Take  $\mathbf{y} = I^{k-2} \mathbf{x}$ . We have

$$\mathbf{y} = L^N(\mathbf{y}) = (\lambda + I)^N(\mathbf{y}) = \lambda^N \mathbf{y} + NI(\mathbf{y}) + 0 = \mathbf{y} + NI(\mathbf{y}) \neq \mathbf{y}.$$

Contradiction. Hence  $I\mathbf{x} = 0$ .

This proof is founded on the classification theorem which I will be happy to tell here:  
Formulate and prove the general classification Theorem.

let  $L$  be a linear operator on  $n$ -dimensional vector space  $V$ . Consider its characteristic polynomial

$$P(t) = \det t - L = \prod_k (t - \lambda_k)^{r_k}, \sum r_k = n.$$

To every root  $\lambda_i$  one can assign at least one non-zero eigenvector  $\mathbf{e}_i$ . If  $r_i \neq 1$ , then situation is not so simple.

We assign to complex number  $\lambda$  the generalised eigenspace  $V_\lambda$ , the set

$$V_\lambda = \{x: N \text{ such that } (L - \lambda)^N = 0\}$$

(One can easy to prove that  $V_\lambda$  is a set).

**Exercise**

$$\lambda \in \{\lambda_i\} \Leftrightarrow V_\lambda \neq 0.$$

Now we represent  $V_i$  as a direct sum of spaces

$$V = \oplus_k V_{\lambda_k}, \quad \dim V_{\lambda_k} = r_k$$

Every subspace is corresponding to eigenvalue  $\lambda_i$ . Operator  $L$  is a direct sum of operators  $L_i$ , such that every  $L_i$  acts on  $V_i$ , and it is a sum on Jordan cells on  $V_i$ . If Polynomial  $P(t)$  is minimal then all  $V_i$  are non-reducible Jordan cells.

Before doing this consider the the problem of decomposition of fraction  $\frac{1}{P(t)}$  on elementary fractions:

We will do this decomposition.

Denote by

$$L_i = \prod_{\lambda_m \neq \lambda_i} (L - \lambda_m)$$

Let  $L$  be linear operator on  $V$ ,  $\dim V < \infty$  such that  $L^n = 1$ . We suppose that  $V$  is over algebraically closed field. (In fact it is enough if  $V$  is defined over cyclotomic subfield.)

P Let  $\{\lambda_i\}$  be set of eigenvalues of  $L$ , set of roots of polynomial

$$P(t) = \det(t - L) = \prod_i (t - \lambda_i)^{r_i}$$

For eigenvalues which do not coincide,  $r_i = 1$ , everything is simple.

To every eigenvalue  $\lambda_i$  one corresponds at least one eigenvector  $\mathbf{e}_k$ :  $L\mathbf{e}_k = \lambda_k\mathbf{e}_k$ ,  $\lambda_k = e^{\frac{2\pi i s_k}{n}}$ , since  $L^n = 1$ .



Let eigenvalue  $\lambda$  ( $\lambda = e^{\frac{2\pi i s_k}{n}}$ ) be degenerate:  $P(t) = (t-a)^m F(t)$ , where  $F(\lambda) \neq 0$ . We want to show that there are exactly  $m$  linearly independent eigenvectors with eigenvalue  $\lambda$ .

Denote  $V_\lambda$  the set of root vectors of  $V$  which correspond to  $\lambda$ :

$$V_\lambda = \{\mathbf{x}: \exists N \text{ such that } (L - \lambda \mathbf{x})^N = 0\}$$

It is evident that  $V_\lambda$  is vector space. We say that  $V_\lambda$  is generalised vector space corresponding to value  $\lambda$ .