Applying Galois Theory to Elementary Problems. Examples

§ 1. How to calculate $\sin 6^\circ$

First of all try to find polynomial (with rational coefficients) such that $\sin 6^\circ$ is its root. Notice that $6 \cdot 5 = 30$ and $\sin 30^\circ = \frac{1}{2}$. Hence express $\sin 30^\circ$ via $\sin 6^\circ$:

$$\sin 5\varphi = \sin 3\varphi \cos 2\varphi + \cos 3\varphi \sin 2\varphi = 16 \sin^5 \varphi - 20 \sin^3 \varphi + 5 \sin \varphi \,. \tag{1}$$

We come to the polynomial equation for $u = \sin 6^\circ$:

$$16u^5 - 20u^3 + 5u = \sin 30^\circ = \frac{1}{2} \,. \tag{2}$$

(We use here trigonometric formulae: $\sin 3\varphi = 3 \sin \varphi - 4 \sin^3 \varphi$ and $\cos 3\varphi = 4cos^3\varphi - 3 \cos \varphi$.)

We do not hope to solve it in radicals straightforwardly. Try to attack it using elementary tools of Galois theory. It is evident from (1) and (2) that if $u = \sin \varphi$ is a root of (2) then $u' = \sin(\varphi + \frac{2\pi}{5})$ is a root of this equation too: $\sin 5(\varphi + \frac{2\pi}{5}) = \sin(5\varphi + 2\pi) = \sin 5\varphi$. Hence it is easy to find all five roots of the polynomial (2) using trigonometric functions:

$$\begin{aligned}
u_1 &= \sin 6^\circ \,, \\
u_2 &= \sin(6^\circ + \tfrac{360^\circ}{5}) = \sin 78^\circ = \cos 12^\circ \,, \\
u_3 &= \sin(6^\circ + 2 \cdot \tfrac{360^\circ}{5}) = \sin 150^\circ = \tfrac{1}{2} \,, \\
u_4 &= \sin(6^\circ + 3 \cdot \tfrac{360^\circ}{5}) = \sin 222^\circ = -\cos 48^\circ \,, \\
u_5 &= \sin(6^\circ + 4 \cdot \tfrac{360^\circ}{5}) = \sin 294^\circ = -\cos 24^\circ \,.
\end{aligned} \tag{3}$$

One of the roots of this polynomial is a rational number, hence the polynomial $16u^5 - 20u^3 + 5u - \frac{1}{2}$ in (2) is reducible over $\mathbf{Q}$: it has linear factor $u - \frac{1}{2}$.

It is more convenient (for calculations) to consider a new variable $t = 2u$. We rewrite our polynomial as

$$\frac{1}{2}t^5 - \frac{5}{2}t^3 + \frac{5}{2}t - \frac{1}{2} = \frac{1}{2}\left(t^5 - 5t^3 + 5t - 1\right) \,. \tag{4}$$

This polynomial has a root $t = 2u = 1$. Thus it contains the linear factor $t - 1$:

$$\frac{1}{2}\left(t^5 - 5t^3 + 5t - 1\right) = \frac{1}{2}(t-1)P_4(t)\,,$$

where

$$P_4(t) = t^4 + t^3 - 4t^2 - 4t + 1\,. \tag{5a}$$

We come to a four order equation:

$$P_4(t) = t^4 + t^3 - 4t^2 - 4t + 1 = 0\,. \tag{5b}$$

for $t = 2\sin 6°$. It follows from (3) that its roots t_1, t_2, t_3, t_4 are

$$< 2\sin 6°, 2\cos 12°, -2\cos 24°, -2\cos 48° > \;. \tag{6}$$

It can be straightforwardly checked that the polynomial $P_4(t)$ is irreducible over $\mathbf{Q}$.

A splitting field of the polynomial P_4 (a minimal field that contains all the roots of this polynomial) is $\Sigma(P_4) = \mathbf{Q}(\sin 6°, \cos 12°, \cos 24°, \cos 48°)$.

First calculate the degree of extension $[\Sigma(P_4) : \mathbf{Q}]$. Notice that $\cos 12° = 1 - 2\sin^2 6°$, $\cos 24° = 2\cos^2 12° - 1$, $\cos 48° = 2\cos^2 24° - 1$, $-\sin 6° = 2\cos^2 48° - 1$.

We see that rational transformation

$$t \mapsto 2 - t^2 \tag{7}$$

transforms roots of P_4 to another roots. This transformation defines $\mathbf{Q}$-automorphism σ of the field $\Sigma(P_4)$ such that:

$$\sigma(t_1) = t_2, \quad \sigma(t_2) = t_3, \quad \sigma(t_3) = t_4, \quad \sigma(t_4) = t_1\,. \tag{8}$$

From (7) and (8) it is evident that all roots belong to field $\mathbf{Q}(t_1) = \mathbf{Q}(\sin 6°)$ ($t_3 = \sigma^2(t) = 2-(2-t)^2$, $t_4 = 2-(2-(2-t)^2)^2$). Hence splitting field $\Sigma(P_4)$ for irreducible polynomial $P_4(t)$ ($\Sigma(P_4) = \mathbf{Q}(t_1, t_2, t_3, t_4)$) is nothing but simple extension $\mathbf{Q}(\sin 6°) : \mathbf{Q}$:

$$\Sigma(P_4) = \mathbf{Q}(t_1, t_2, t_3, t_4) = \mathbf{Q}(\sin 6°) \quad \text{and} \quad [\Sigma(P_4) : \mathbf{Q}] = [\mathbf{Q}(\sin 6°) : \mathbf{Q}] = 4\,. \tag{9}$$

This extension is normal extension of degree 4. Hence Galois group of polynomial (5) (group of automorphisms of the field $\mathbf{Q}(\sin 6°) = \Sigma(P_4(t))$ contains precisely 4 elements:

$$G = \Gamma(\Sigma : \mathbf{Q}) = \{1, \sigma, \sigma^2, \sigma^3\}\,, \tag{10}$$

where σ is automorphism (8).

This group is abelian cyclic group: $\sigma^4 = 1$. It contains only one proper subgroup H ($H \neq 1$, $H \neq G$):

$$H = \{1, \sigma^2\}, \quad |H| = 2 .$$

To subgroup H corresponds intermediate field $M = H^\dagger$: $M = H^\dagger$ is maximal subfield in $Q(\sin 6^\circ)$ such that its elements are invariant under transformations from H, i.e. under transformation σ^2:

$$\mathbf{Q} \subset M \subset \mathbf{Q}(\sin 6^\circ), \quad M = \{a \in \mathbf{Q}(\sin 6^\circ) \text{ such that } \sigma^2(a) = a\} ,$$

$$[\mathbf{Q}(\sin 6^\circ) : M] = 2, \quad [M : \mathbf{Q}] = 2 . \tag{11}$$

Intermediate extensions are quadratic (degree is equal to 2). Hence every element of field $\mathbf{Q}(\sin 6^\circ)$ and in particularly $\sin 6^\circ$ is a root of **quadratic polynomial with coefficients in** M. This quadratic polynomial is reducible over M iff the element belongs to the intermediate field M [1)]. In the same way coefficients of this quadratic polynomial are roots of quadratic polynomials with rational coefficients. Hence we can calculate every element of the field $\mathbf{Q}(\sin 6^\circ)$ and in particularly $\sin 6^\circ$ solving two quadratic equations.

Perform these calculations.

Find first quadratic polynomial with coefficients in M such that $\sin 6^\circ$ is its root. Consider elements α and β in $\mathbf{Q}(\sin 6^\circ)$ such that

$$\begin{aligned} \alpha &= t_1 + t_3 = t_1 + \sigma^2 t_1 , \\ \beta &= t_1 \cdot t_3 = t_1 \cdot \sigma^2 t_1 , \end{aligned} \tag{12}$$

where t_1, t_2, t_3, t_4 are roots (6) of polynomial $P_4(t)$.

It is evident from (12) that $t_1 = 2\sin 6^\circ$ and $t_3 = -2\cos 24^\circ$ are roots of the following quadratic polynomial

$$P_2(t) = t^2 - \alpha t + \beta . \tag{13}$$

[1)] If $[L : K] = 2$ then for arbitrary $a \in L$ elements $1, a, a^2$ are linear dependent over field K, hence there exist coefficients $p, q, r, \in K$ such that not all are equal to zero and relation $p + qa + ra^2 = 0$ is obeyed.

On the other hand one can see from (8) that $\sigma^2(\alpha) = \alpha$ and $\sigma^2(\beta) = \beta$. Hence elements α and β belong to intermediate field M, because they do not change under the action of automorphism σ^2.

We see that quadratic polynomial (13) with coefficients α and β in the field M is just required quadratic polynomial with coefficients in M: $P_2(\sin 6^{\circ}) = 0$.

It remains to calculate α and β which belong to field M. M is quadratic extension of $\mathbf{Q}$ ($[M : \mathbf{Q}] = 2$). Thus $\alpha \in M$ and $\beta \in M$ are roots of quadratic polynomial with rational coefficients.

It follows from (6) and (12) and elementary stuff of trigonometric formulae that

$\alpha = t_1 + t_3 = 2\sin 6^\circ - 2\cos 24^\circ =$

$$= 2\sin 6^\circ - 2\sin 66^\circ = 4\sin\frac{6-66}{2}\cos\frac{6+66}{2} = -2\cos 36 = 4\sin^2 18^\circ - 2 \qquad (14a)$$

and $\beta = t_1 \cdot t_3 =$

$$2\sin 6^\circ \cdot (-2\cos 24) = -4(\sin 6^\circ \cos 24^\circ) = -2(\sin 30^\circ - \sin 18^\circ) = 2\sin 18^\circ - 1\,. \qquad (14b)$$

We see from these relations that

$$M = \mathbf{Q}(\sin 18^\circ)\,.$$

In particularly this means that $\sin 18^\circ$ is a root of quadratic polynomial with rational coefficients. So instead calculating α and β as roots of quadratic polynomials we calculate just $\sin 18^{\circ}$ as a root of quadratic polynomial and express α and β via $\sin 18^{\circ}$.

Find this quadratic polynomial with rational coefficients for $\sin 18^\circ$. One can see that $\sin 18^\circ$ is a root of polynomial $4t^2 + 2t - 1$:

$$4\sin^2 18^\circ + 2\sin 18^\circ - 1 = 0\,. \qquad (15)$$

Hence

$$\sin 18^\circ = \frac{\sqrt{5}-1}{4}\,.$$

Remark 1 There are many ways to obtain relation (15). Not the most beautiful one but right one is the following:

$0 = \cos 36^\circ - \sin 54^\circ = (1 - 2\sin^2 18) - (3\sin 18^\circ - 4\sin^3 18^\circ) =$

$$4\sin^3 18^\circ - 2\sin^2 18^\circ - 3\sin 18^\circ + 1 = (\sin 18^\circ - 1)(4\sin^2 18^\circ + 2\sin 18^\circ - 1)\,.$$

Remark 2. The number $\tau = 2\sin 18^\circ = \frac{\sqrt{5}-1}{2}$ is so called "golden ratio". It has many wonderful properties... One of the ways to obtain relation (15) straightforwardly as relation for golden ratio is to consider triangle with angles $(72^\circ, 72^\circ, 36^\circ)$ and bisect the angle 72°.

Now from (14) and (15) it follows that

$$\alpha = 4\sin^2 18^\circ - 2 = -2\sin 18^\circ - 1 = -\frac{1+\sqrt{5}}{2}\,.$$

$$\beta = 2\sin 18^\circ - 1 = \frac{\sqrt{5}-3}{2} \qquad (16)\,.$$

.

So from (13) and (16) it follows that $t_1 = 2\sin 6^\circ$ and $t_3 = -2\cos 24^\circ$, are roots of quadratic equation

$$t^2 + \frac{1+\sqrt{5}}{2}t - \frac{3-\sqrt{5}}{2} = 0\,. \qquad (17)$$

$$t_{1,2} = \frac{\pm\sqrt{30-6\sqrt{5}} - \sqrt{5} - 1}{4}$$

Positive root of this equation is equal just to $t_1 = 2\sin 6^\circ$ and

$$\sin 6^\circ = \frac{\sqrt{30-6\sqrt{5}} - \sqrt{5} - 1}{8} \qquad (18)$$

We calcualted $\sin 6^\circ$!

§ 2.Angles that can be constructed by ruler and compass. Why 50 pence coin has 7 edges?

We see from (18) that $\sin 6^\circ$ (so and $\cos 6^\circ$) is expressed trough rational numbers with additional operation $\sqrt{}$ of taking square root. It means that we can construct by ruler and compass the angle 6°, i.e. we can divide the circle by ruler and compass on 60 equal arcs.[2)]

The reason why it happens is obvious. The degree of normal extension $\mathbf{Q}(\sin 6^\circ) : \mathbf{Q}$ is equal to $4 = 2 \times 2$. Hence elements of intermediate field M in (11) are expressed through

[2)] Operations with rational numbers: multiplication, addition substraction and division and operation of taking of square root are possible with ruler and compass: If a and b are segments on the line and c is segment corresponding to unity then one can construct by ruler and compass the segments $a+b$, $a-b$, $\frac{ab}{c}$, $\frac{ac}{b}$ and $\sqrt{ab}$.

elements of field $\mathbf{Q}$ with square root operation and elements of $\mathbf{Q}(\sin 6^\circ)$ are expressed through elements of field M with square root operation.

Now we consider a more general situation.

Definition We say that complex number a is *quadratic irrationality*it is better to call iteraed quadratic irrationalityf it belongs to the field L such that it can be included in a tower of quadratic extensions:

$$\mathbf{Q} = M_0 \subseteq M_1 \subseteq M_2 \subset \ldots \subseteq M_n = L\,, \quad [M_{k+1} : M_k] \leq 2 \text{ for every } k = 0, 1, \ldots, n-1\,. \tag{2.1}$$

It is evident that the set of quadratic irrationalities (including usual rational numbers) is a field.

For example the number $\alpha = \sqrt{3} + \sqrt{2 + \sqrt{5 + \sqrt{7}}}$ is quadratic irrationality because the field $\mathbf{Q}(\alpha)$ can be included in the following tower

$$\mathbf{Q} \subseteq \mathbf{Q}\left(\sqrt{7}\right) \subseteq \mathbf{Q}\left(\sqrt{5+\sqrt{7}}\right) \subseteq \mathbf{Q}\left(\sqrt{2+\sqrt{5+\sqrt{7}}}\right) \subseteq \mathbf{Q}\left(\sqrt{3}, \sqrt{2+\sqrt{5+\sqrt{7}}}\right) \tag{2.2}$$

and all these extensions are evidently quadratic.

The number $\sin 6^\circ$ is quadratic irrationality because for the tower (11) extensions $M : \mathbf{Q}$ and $\mathbf{Q} : \mathbf{Q}(\sin 6^\circ)$ are quadratic.

If number is quadratic irrationality then from (2.1) it follows that it can be expressed via rational numbers with taking square root operation: every number in M_n is a root of quadratic equation with coefficients in M_{n-1}, coefficients in M_{n-1} are roots of quadratic equation with coefficients in M_{n-2} and so on.

We say that angle φ is constructive if it can be constructed by ruler and compass. Angle φ is constructive if and only if $\sin\varphi$ is quadratic irrationality. (Evidently $\cos\varphi = \pm\sqrt{1-\sin^2\varphi}$ is quadratic irrationality iff $\sin\varphi$ is quadratic irrationality.) The circle can be divided on N equal arcs by ruler and compass if and only if the angle $\frac{2\pi}{N}$ is constructive.

We know from school that for $N = 2, 3, 4, 6$, $N = 2^k$ circle can be divided on N equal parts by ruler and compass. ($\sin 45^\circ = \frac{\sqrt{2}}{2}$, $\sin 60^\circ = \frac{\sqrt{3}}{2}$, $\sin\frac{2\pi}{2^{k+1}} = \sqrt{\frac{1-\cos\frac{2\pi}{2^k}}{2}}$ are quadratic irrationalities).

ratic irrationality i

In the previous Section we proved in fact that for all N such that N divides 60, circle can be divided on N equal parts by ruler and compass: If $Nk = 60$ then $\sin \frac{2\pi}{N}$ is quadratic irrationality because $\sin \frac{2\pi}{N} = \sin \frac{2\pi}{60} k = \sin k \cdot 6^\circ$.

Now we describe all N such that $\sin \frac{2\pi}{N}$ is quadratic irrationality, i.e. all N such that circle can be divided on N equal arcs by ruler and compass[3)].

Consider the complex number

$$\varepsilon_N = \exp\left(\frac{2\pi i}{N}\right), \tag{2.3}$$

where $N = 1, 2, 3, \dots$ is an arbitrary positive integer.

We study this complex number instead $\sin \frac{2\pi}{N}$. The number ε_N is quadratic irrationality if and only if $\sin \frac{2\pi}{N}$ is quadratic irrationality ($\sin \varphi = \frac{\exp(i\varphi) - \exp(-i\varphi)}{2i}$, $\exp(i\varphi) = \cos \varphi + i \sin \varphi$).

The field extension $\mathbf{Q}(\varepsilon_N) : \mathbf{Q}$ is finite normal extension, because it is splitting field for polynomial $t^N - 1$. (The roots of this polynomial are $\{1, \varepsilon_N, \varepsilon_N^2, \dots, \varepsilon_N^{N-1}\}$.) So from fundamental theorem of Galois theory it follows that number of elements in Galois group of field extension $\mathbf{Q}(\varepsilon_n) : \mathbf{Q}$ is equal to the degree of this extension:

$$|\Gamma(\mathbf{Q}(\varepsilon_N) : \mathbf{Q})| = [\mathbf{Q}(\varepsilon_N) : \mathbf{Q}]\,. \tag{2.4}$$

For the considerations below we need the following two lemmas.

Lemma 1 *Consider the decomposition of N in prime factors:*

$$N = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}\,. \tag{2.5}$$

Then for normal extension $\Gamma(\mathbf{Q}(\varepsilon_N) : \mathbf{Q})$ the degree of this extension and correspondingly the number of elements in Galois group $\Gamma(\mathbf{Q}(\varepsilon_N) : Q)$ are given by the following formula:

$$|\Gamma(\mathbf{Q}(\varepsilon_N) : Q)| = [\mathbf{Q}(\varepsilon_N) : Q] = (p_1 - 1)p_1^{n_1 - 1}(p_2 - 1)p_2^{n_2 - 1} \dots (p_k - 1)p_k^{n_k - 1}\,. \tag{2.6}$$

[3)] The problem of dividing of circle on N equal arcs with ruler and compass was posed by ancient Greeks. They knew the answer for $N = 3, 5, 15$. Also they knew the answer for $N = 2k$ provided there exists an answer for $N = k$ (obvious method of bisecting the angle). For about two thousands year little progress was made beyond the Greeks. On 30 March 1796, Gauss made the remarkable discovery: he solved this problem for $N = 17$. He was nineteen years old at the time. So pleased was he with this discovery that he resolved to dedicate the rest of his life to mathematics.

Lemma 2 *If finite group G contains 2^k elements then for this group there always exists the sequence $\{G_0, G_1, \ldots, G_k\}$ of subgroups such that $G_k = G$, $G_0 = 1$ and G_i is subgroup of the index 2 in the subgroup G_{i+1} ($i = 0, 1, 2, \ldots, k-1$):*

$$1 = G_0 < G_1 \ldots < G_k = G, \quad |G_{k+1}| : |G_k| = 2\,. \tag{2.7}$$

We prove these lemmas in the end. Now we use these lemmas for studying necessary and sufficient conditions for ε_N be quadratic irrationality.

If ε_n is quadratic irrationality then from definition (2.1) and "Tower Law" it follows that degree of normal extension $\mathbf{Q}(\varepsilon_n) : Q$ is equal to the $[\mathbf{Q}(\varepsilon_n) : M_{n-1}] \cdot [M_{n-1} : M_{n-2}] \cdots [M_1 : \mathbf{Q}] = 2^k$ for some positive integer k. On the other hand from Lemma 2 it follows that if degree (2.6) of normal extension $\mathbf{Q}(\varepsilon_N) : Q$ is equal to the power of 2 ($[\mathbf{Q}(\varepsilon_N) : Q] = 2^k$) then ε_N is quadratic irrationality. Namely consider the sequence of subgroups (2.7). The extension $\mathbf{Q}(\varepsilon_N) : \mathbf{Q}$ is normal extension and according to Fundamental theorem of Galois theory to this sequence of subgroups correspond the tower of field extensions:

$$\mathbf{Q} = G^\dagger = G_k^\dagger \subset G_{k-1}^\dagger \subset \ldots \Gamma_1^\dagger \subset G_0^\dagger = \mathbf{Q}(\varepsilon_N) \tag{2.8}$$

Here we denote by G the Galois group $\Gamma(\mathbf{Q}(\varepsilon_N) : \mathbf{Q})$, for the subgroup G_i as usually we denoted by $G_i^\dagger$ the subfield of all elements of the field $\mathbf{Q}(\varepsilon_n)$ that do not change under the action of elements of subgroup G_i ($G_i^\dagger = \{a\colon \quad \forall g \in G_i\, g(a) = a\}$).

Note that all subgroups G_i are normal subgroups in G_{i+1} because their index is equal to 2. This corresponds to the fact that every extension of degree 2 is normal [3)]. The Galois correspondence gives that all extensions $G_{i-1}^\dagger : G_i^\dagger$ are quadratic extensions: $[G_{i-1}^\dagger : G_i^\dagger] = |G_i / G_{i-1}| = |G_i| : |G_{i-1}| = 2$. Hence ε_N is quadratic irrationality.

[3)] We note that in the case if σ is an automorphism of field L such that $\sigma \neq 1$ and $\sigma^2 = 1$ and K is subfield of elements that do not change under σ (Galois group of extension $L : K$ contains exactly two elements $\{1, \sigma\}$) then one can explicitly describe the field L in terms of field K: Consider arbitrary $a \in L/K$ and element $s = a - \sigma(a)$. $\sigma(s) = -s$, $s^2 \in K$ and $s \neq 0$. For every element x in L $x_1 = x + \sigma(x) \in K$ and $x_2 = s(x - \sigma(x)) \in K$ because $\sigma(x_1) = x_1, \sigma(x_2) = x_2$. Hence $x = x_1/2 + s^{-1}x_2/2$. $L = K(s)$, where s a square of polynomial $t - s^2$.

We see that ε_N is quadratic irrationality if and only if the degree (2.6) of normal extension $\mathbf{Q}(\varepsilon_N) : \mathbf{Q}$ is equal to the power of 2 ($[\mathbf{Q}(\varepsilon_N) : \mathbf{Q}] = 2^k$). To find such N we apply Lemma 1.

It is obvious that the right hand side of (2.6) is equal to the power of 2 if and only if the following conditions hold:

1) all $n_i \leq 1$ for $p_i \neq 2$, i.e. N is a product of power of 2 on the different odd prime numbers.

2) all odd primes p, factors of N obey to condition that $p-1$ is a power of 2.

Prime number p obeying to the condition that $p - 1 = 2^m$ is called Fermat prime numbers (or sometimes they are called Messner prime numbers). It is evident that if p is prime number and $p-1 = 2^m$ then m is also power of 2. (If $m = 2^r q$, where q is odd, then p contains the factor $2^{2^r} + 1$). So Fermat prime number is a prime number p such that

$$p = 2^{2^r} + 1\,. \tag{2.9}$$

E.g. $p = 3, 5, 17, 257$ are Fermat prime numbers [4].

Thus we come to Theorem:

Theorem For the integer N the number $\sin \frac{2\pi}{N}$ is quadratic irrationality and correspondingly circle can be divided on N equal arcs by ruler and compass if and only if the decomposition of N in prime factors have the following form

$$N = 2^k p_1 \dots p_s\,,$$

where all $p_1, \dots, p_s$ are different Fermat prime numbers.

For example circle can be divided on 60 parts. Circle cannot be divided on 7,9,11 parts. ($60 = 2^2 \cdot 3 \cdot 3 \cdot 5$, 3 and 5 are Fermat primes, $9 = 3^2$ it is square of odd prime, 7 and 11 are not Fermat primes)

We see that 7 is the smallest number such that circle cannot be divided on the 7 parts with ruler and compass. May be it is the reason why 50 pence coin has 7 edges?..

Finally we prove the Lemmas.

Proof of the Lemma 1.

[4] Fermat conjectured that numbers (2.5) are prime for all n. This is wrong.

In the case if $N = p$ is simple number then ε_p is a root of irreducible polynomial $1 + t + \ldots + t^{p-1}$ of degree $p - 1$ and we come to (2.6).

In the general case it is easier to calculate Galois group.

Consider the ring $\mathbf{Z}/N\mathbf{Z}$ corresponding to the roots $1, \varepsilon_N, \varepsilon_N^2 \ldots, \varepsilon_N^{N-1}$. The Galois automorphism are in one-one correspondence with invertible elements of this ring: if r is invertible element of the ring $\mathbf{Z}/NZ$ (i.e. r and N are coprime) then transformation $\varepsilon_N \mapsto \varepsilon_N^r$ defines automorphism $\sigma_r \in \Gamma(\mathbf{Q}(\varepsilon_N) : \mathbf{Q})$. To every automorphism $\sigma \in \Gamma(\mathbf{Q}(\varepsilon_N) : \mathbf{Q})$ such that $\sigma(\varepsilon_N) = \varepsilon_N^r$ corresponds element r and r is invertible because if $\sigma(\varepsilon_N^{-1}) = \varepsilon_N^q$ then $rq = 1(mod\, N)$. Hence the number of elements in Galois group $\Gamma(\mathbf{Q}(\varepsilon_N) : \mathbf{Q})$ is equal to number of positive integers r such that $r < N$ and r and N are coprime. This number is evidently equal to r.h.s. of (2.6). Lemma is proved.

Proof of the Lemma 2

Prove it by induction. For $|G| = 2$ proof is evident.

Suppose that we already prove the Lemma for $m \leq k$ ($|G| = 2^m$).

Consider finite group containing 2^{k+1} elements.

First prove that there exist in G element a such that it commutes with all elements in G.

Consider for every element h of this group the subgroup N_h stabilizer of this element and class $\mathcal{O}_h$ of all conjugated elements

$$N_h = \{g \in G: \quad ghg^{-1} = h\}\,, \quad \mathcal{O}_h = \{ghg^{-1}, g \in G\}\,.$$

($\mathcal{O}_h$ is the orbit of h under adjoined action of the group G).

It is evident that

$$|N_h| \cdot |\mathcal{O}_h| = 2^{k+1}\,, \tag{2.7}$$

i.e. number of elements in the every class is equal to the index of corresponding subgroup.

Let $h_1, \ldots h_m$ are all representatives of all classes of conjugated elements.

It follows from (2.7) that every class $\mathcal{O}_{h_i}$ contains $2^{q(h_i)}$ elements. $2^{q(h_1)} + \ldots + 2^{q(h_m)} = 2^{k+1}$ Class of unity contains one element. Hence there exists another class which contains one element too. Thus there exists an element a such that $|\mathcal{O}_a| = 1$, i.e. $ag = ga$, $\forall g \in G$. Considering the set $\{1, a, a^2, \ldots\}$ we come to cyclic subgroup $1, a, a^2, \ldots, a^{r-1}$ generated by a. This subgroup (like every subgroup of G) contains power of 2 ($r = 2^t$) elements.

Consider element $c = a^{\frac{r}{2}}$. This element obviously commutes with all elements in G and $c^2 = 1$. Thus we come to the subgroup $H = \{1, c\}$ such that this subgroup is normal subgroup. Consider group $G' = G/H$. This group contains 2^k elements and by inductive hypothesis there exists the sequence

$$1 = G'_0 < \ldots < G'_k = G' = G/H \tag{2.8}$$

obeying to condition (2.6).

Consider now subgroups G_k in G such that $G_0 = H$, and all G_k $(k \geq 1)$ are subgroups of G such that $G_k/H = G'_{k-1}$. $(G_k = G'_{k-1} \cup cG'_{k-1})$ Then we come to the sequence

$$1 = G_0 < G_1 < \ldots < G_{k+1} = G$$

which obeys to Lemma 2.

Lemma is proved.