Lecture Notes On Abstract Algebra (Week 15)

Guohua PENG (彭国华)
email: peng@scu.edu.cn

Contents

1 Lecture 28 (Dec 12, 2023): Galois Correspondence

Galois Theory uncovers a relationship between the structure of groups and the structure of fields. It then uses this relationship to describe how the roots of a polynomial relate to one another. Galois theory is named after a French mathematician Evariste Galois (1811-1832) who did some very important work in this area. He had a very dramatic and difficult life, failing to get much of his work recognised due to his great difficulty in expressing himself clearly. For example, he wasn't admitted to the leading university in Paris, the Ecole Polytechnique, and had to make do with the Ecole Normale. He also met with difficulty because of his political sympathies, he was a republican. This led to him being expelled from the Ecole Normale when he wrote a letter to a newspaper criticising the director of the school. He joined a republican branch of the militia and was later imprisoned (twice) because of his membership. The second time whilst in prison he fell in love with the daughter of the prison physician, Stephanie-Felice du Motel and after being released died in a duel with Perscheux d'Herbinville. The reasons for the duel are not entirely clear, but it seems likely it had something to do with Stephanie. His death started republican riots and rallies which lasted for several days.

Although Galois is often credited with inventing group theory and Galois theory, it seems that an Italian mathematician Paolo Ruffini (1765-1822) may have come up with many of the ideas first. Unfortunately his ideas were not taken seriously by the rest of the mathematical community at the time.

1.1 Fundamental Theorem of Galois Theory

Corollary 1.1. *Let K/F be a finite Galois extension with Galois group G. Let M be an intermediate field of K/F. Then the field extension K/M is Galois and*

$$\mathrm{Gal}(K/M) = \{g \in G \mid g(x) = x, \forall x \in M\} = \{g \in G \mid g|_M = \mathrm{id}_M\}.$$

$$\begin{array}{cc} K & 1 \\ | & | \\ M & H = \mathrm{Gal}(K/M) \\ | & | \\ F & G \end{array}$$

Proof. It's obvious that K/M is a Galois extension. Let $H = \{g \in G \mid g|_M = \mathrm{id}_M\}$. Since $\mathrm{Gal}(K/M)$ is a subgroup of G and the restriction of every element in $\mathrm{Gal}(K/M)$ on M is the identity map, we have $\mathrm{Gal}(K/M) \subseteq H$. On the other hand, every element in H is an M-automorphism on K, hence $H \subseteq \mathrm{Gal}(K/M)$. So $H = \mathrm{Gal}(K/M)$. □

Basic Observation

1. For $H \leq \mathrm{Aut}(K)$ and $\sigma \in \mathrm{Aut}(K)$, then $K^{\sigma H \sigma^{-1}} = \sigma(K^H)$.
2. If $H_1 \leq H_2 \leq \mathrm{Aut}(K)$, then $K^{H_2} \subseteq K^{H_1}$.
3. If $F \subseteq L_1 \subseteq L_2 \subseteq K$, then $\mathrm{Gal}(K/L_2) \subseteq \mathrm{Gal}(K/L_1)$.

$$\begin{array}{cc} 1 & K \\ | & | \\ H & \longmapsto K^H \\ | & | \\ G & F \end{array} \qquad \begin{array}{cc} K & 1 \\ | & | \\ L & \longmapsto H = \mathrm{Gal}(K/L) \\ | & | \\ F & G \end{array} \qquad \begin{array}{cc} K & 1 \\ | & | \\ L_2 & H_2 = \mathrm{Gal}(K/L_2) \\ | & | \\ L_1 & H_1 = \mathrm{Gal}(K/L_1) \\ | & | \\ F & G \end{array}$$

Theorem 1.1 (**Fundamental Theorem of Galois Theory**, **伽罗瓦理论的基本定理**). *Let K/F be a finite Galois extension with Galois group G.*

1. *There is a one-to-one inclusion reversing correspondence between subgroups of G and intermediate fields of the field extension K/F.*

   More precisely, let $\mathcal{S}$ be the set of all subgroups of G and $\mathcal{M}$ the set of all intermediate fields of the field extension K/F, then the following map

   $$\begin{aligned} \iota : \mathcal{S} &\to \mathcal{M} \\ H &\mapsto K^H \end{aligned}$$

   is a bijection such that

   (1) the inverse image of $L \in \mathcal{M}$ is $\mathrm{Gal}(K/L) : \iota^{-1}(L) = \mathrm{Gal}(K/L)$; and

   (2) for $H_1, H_2 \in \mathcal{S}$, $H_1 \subseteq H_2$ if and only if $K^{H_2} \subseteq K^{H_1}$, i.e. $\iota(H_2) \subseteq \iota(H_1)$.

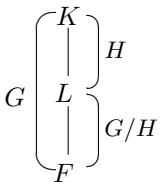
2. *Let L be an intermediate field of K/F. Then the extension L/F is Galois if and only if $H = \mathrm{Gal}(K/L)$ is a normal subgroup of G.*

If L/F is normal (hence Galois), the restriction map

$$\begin{aligned} \mathrm{res} : G &\to \mathrm{Gal}(L/F) \\ \sigma &\mapsto \sigma|L \end{aligned}$$

determines an epimorphism of groups from G onto $\mathrm{Gal}(L/F)$ with kernel H. In particular,

$$\mathrm{Gal}(L/F) \cong G/H.$$



Proof. 1. The injection of ι is a direct consequence of Corollary **??**. The surjection of ι is also a consequence of Theorem **??**, since K/L is Galois for $L \in \mathcal{M}$.

It follows from the definition of fixed field and Galois group that the correspondence is inclusion-reversing: $H_1 \subseteq H_2$ implies $K^{H_2} \subseteq K^{H_1}$; $L_1 \subseteq L_2$ implies $\mathrm{Gal}(K/L_2) \subseteq \mathrm{Gal}(K/L_1)$.

2. Firstly, for any intermediate field L, K/L is Galois and L/F is separable. Set $H = \mathrm{Gal}(K/L)$.

Notice that the extension L/F is normal if and only if $\sigma(L) = L$ holds for every F-embedding from L to $\overline{L} = \overline{F}$, an algebraic closure of F.

It's obvious that the restriction of an automorphism in G to L is an F-embedding from L into K. Conversely, if σ is an F-embedding from L into $\overline{F}$, then σ extends to an F-embedding from K into $\overline{F}$, hence an F-automorphism of K and $\sigma(L) \subseteq \sigma(K) = K$, since K/F is normal. Thus each F-embedding on L comes from the restriction of an element of G to L. It follows that L/F is a normal extension if and only if $\sigma(L) = L$ for every $\sigma \in G$.

One can easily check that for every $\sigma \in G$, $\mathrm{Gal}(K/\sigma(L)) = \sigma H \sigma^{-1}$. By the above one-to-one correspondence, we have L/F is normal if and only if $\sigma H \sigma^{-1} = H$ for every $\sigma \in G$, or equivalently $H \lhd G$.

Now assume $H \lhd G$ (equivalently L/F is a Galois extension). The map "res" is surjective by the argument given above. The kernel is the set of all automorphisms in G whose restrictions to L are the identity map on L, that is, the kernel of the "res" homomorphism is $\mathrm{Gal}(K/L) = H$ (also see Corollary 1.1). Therefore,

$$G/H \cong \mathrm{Gal}(L/F).$$

□

Remark 1.1. 1. Theorem 1.1 is also called the **Main Theorem of Finite Galois Theory**. The correspondence between subgroups and intermediate fields in Theorem 1.1 is also called the **Galois Correspondence** (Galois对应) of field extensions.

2. Galois Theory establishes explicit connections between the intermediate subfields and the subgroups of the whole Galois group.

3. The Fundamental Theorem shows that for an intermediate subfield L of K/F, L/F is normal if and only if the corresponding subgroup $\mathrm{Gal}(K/L)$ is normal in $\mathrm{Gal}(K/F)$. The main steps of the proof may be described as follows.

$$\begin{aligned}
\text{The extension } L/F \text{ is Galois} &\iff L/F \text{ is normal} \\
&\iff \sigma(L) = L \text{ holds for all } F\text{-embeddings on } L \\
&\iff \sigma(L) = L \text{ holds for all } \sigma \in G \\
&\iff \iota^{-1}(\sigma(L)) = \iota^{-1}(L) \text{ holds for all } \sigma \in G \\
&\iff \mathrm{Gal}\,(K/\sigma(L)) = \mathrm{Gal}\,(K/L) \text{ holds for all } \sigma \in G \\
&\iff \sigma^{-1}\mathrm{Gal}\,(K/L)\,\sigma = \mathrm{Gal}\,(K/L) \text{ holds for all } \sigma \in G \\
&\iff \mathrm{Gal}\,(K/L) \text{ is normal in } G.
\end{aligned}$$

Corollary 1.2. *Let K/F be a finite Galois extension with Galois group $G = \mathrm{Gal}(K/F)$.*

1. *There are finitely many intermediate subfields for K/F.*
2. *The intermediate subfields of the field extension K/F correspond to the subgroups of G one by one.*
3. *If H is a subgroup of G, then*

$$[K : K^H] = |H|, \quad [K^H : F] = [G : H] = \frac{|G|}{|H|}.$$

Example 1.1. Let $K = \mathbb{Q}(\zeta_n)$. Then $K/\mathbb{Q}$ is Galois with $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. In fact,

$$G = \mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_a \mid (a, n) = 1, \sigma_a(\zeta_n) = \zeta_n^a\}.$$

For subgroup $H = \{1, \sigma_{-1}\}$, the fixed subfield $K^H = \mathbb{Q}(\zeta_n) + \zeta_n^{-1}) = K^+$, the maximal real subfield of K. And

$$\mathrm{Gal}(K/K^+) = H = \{1, \sigma_{-1}\}, \quad \mathrm{Gal}(K^+/\mathbb{Q}) \cong G/\{1, \sigma_{-1}\} \cong (\mathbb{Z}/n\mathbb{Z})^\times/\{\pm 1\}.$$

1.2 Subfields of $\mathbb{Q}(\sqrt[4]{2}, \sqrt{-1})$

Let $\alpha = \sqrt[4]{2}$ and $K = \mathbb{Q}(\alpha, i)$. Then K is a splitting field of $x^4 - 2$ over $\mathbb{Q}$. Since every subfield of K contains $\mathbb{Q}$ as a subfield, a subfield of K corresponds to an intermediate subfield of the field extension $K/\mathbb{Q}$.

The Galois group of $x^4 - 2$ is $G = \mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle$, where $\sigma(\alpha) = i\alpha, \sigma(i) = i$ and $\tau(\alpha) = \alpha, \tau(i) = -i$. One can find that G has 5 elements of order 2, 2 elements of order 4 and G has 10 subgroups:

$$\begin{aligned}
&H_0 = 1,\ H_1 = \langle \sigma \rangle = \{1, \sigma, \sigma^2, \sigma^3\},\ H_2 = \langle \tau \rangle = \{1, \tau\},\ H_3 = \langle \sigma^2 \rangle = \{1, \sigma^2\}, \\
&H_4 = \langle \sigma\tau \rangle = \{1, \sigma\tau\},\ H_5 = \langle \sigma^2\tau \rangle = \{1, \sigma^2\tau\},\ H_6 = \langle \sigma^3\tau \rangle = \{1, \sigma^3\tau\}, \\
&H_7 = \langle \sigma^2, \tau \rangle = \{1, \sigma^2, \tau, \sigma^2\tau\},\ H_8 = \langle \sigma^2, \sigma\tau \rangle = \{1, \sigma^2, \sigma\tau, \sigma^3\tau\},\ H_9 = G.
\end{aligned}$$

One of them has order 1, five amongst them have order 2, three subgroups have order 4 and one has order 8. The following are their correlations:

$$\begin{aligned}
&H_2 \subset H_7 \lhd G,\ H_3 = C(G) = H_1 \cap H_7 = H_1 \cap H_8 \lhd G, \\
&H_4 \subset H_8,\ H_5 \subset H_7 \lhd G, H_6 \subset H_8 \lhd G.
\end{aligned}$$

It's easy to check that

$$K^{H_1} = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1}), \quad K^{H_2} = \mathbb{Q}(\alpha).$$

By careful investigating the action of $\sigma^r\tau^s$ $(r = 0, 1, 2, 3, s = 0, 1)$, we can obtain that

$$\begin{aligned} &K^{H_0} = K,\ K^{H_3} = \mathbb{Q}(\alpha^2, i) = \mathbb{Q}(\sqrt{2}, \sqrt{-1}),\ K^{H_4} = \mathbb{Q}((1+i)\alpha) \\ &K^{H_5} = \mathbb{Q}(i\alpha),\ K^{H_6} = \mathbb{Q}((1-i)\alpha),\ K^{H_7} = \mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{2}), \\ &K^{H_8} = \mathbb{Q}(i\alpha^2) = \mathbb{Q}(\sqrt{-2}),\ K^{H_9} = \mathbb{Q}. \end{aligned}$$

To achieve K^H for a subgroup H, we my take the following two steps:

1. compute $[K^H : \mathbb{Q}] = [G : H]$.
2. find elements $\beta_1, \beta_2, \ldots, \beta_m \in K$ satisfying $\varphi(\beta_i) = \beta_i$ for every generator φ of H_i so that $K^H = \mathbb{Q}(\beta_1, \beta_2, \ldots, \beta_m)$.

For example, $[K^{H_4} : \mathbb{Q}] = [G : H_4] = 4$, so $K^{H_4}/\mathbb{Q}$ is a field extension of degree 4. Note that $H_4 = \langle\sigma\tau\rangle$ and

$$\begin{aligned} \sigma\tau : K &\to K \\ \alpha &\mapsto \alpha i \\ i &\mapsto -i. \end{aligned}$$

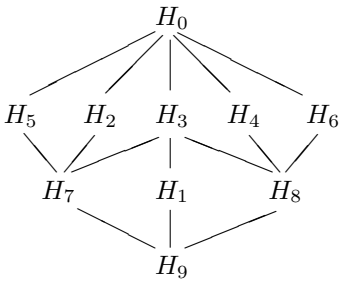
Then $\sigma\tau(\alpha^2) = -\alpha^2$, which implies that $\sigma\tau(\alpha^i) = \alpha^i$. This means $\alpha^2 i \in K^{H_4}$. But $[\mathbb{Q}(\alpha^2 i) : \mathbb{Q}] = 2$, which means $\alpha^2 i$ is not enough to generate K^{H_4}. We need to find one more element which is not in $\mathbb{Q}(\alpha^2 i)$. Since $\sigma\tau(\alpha) = \alpha i, \sigma\tau(\alpha i) = \alpha$, we have $\sigma\tau(\alpha + \alpha i) = \alpha + \alpha i$. Therefore $K^{H_4} = \mathbb{Q}(\alpha^2 i, \alpha(1+i)) = \mathbb{Q}(\alpha(1+i))$.

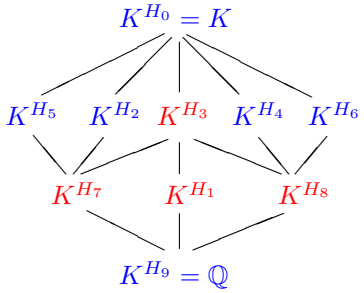
It's easy to verify that $K^{H_3} = K^{H_1}K^{H_7} = K^{H_1}K^{H_8}$ and

$$\begin{aligned} &\mathrm{Gal}(K^{H_1}/\mathbb{Q}) \cong G/H_1 \cong C_2, \quad \mathrm{Gal}(K^{H_3}/\mathbb{Q}) \cong G/H_3 \cong C_2 \otimes C_2, \\ &\mathrm{Gal}(K^{H_7}/\mathbb{Q}) \cong G/H_7 \cong C_2, \quad \mathrm{Gal}(K^{H_8}/\mathbb{Q}) \cong G/H_8 \cong C_2, \end{aligned}$$

where C_2 denotes a cyclic group of order 2.

In summary, we obtain that $K/\mathbb{Q}$ has 8 intermediate subfields except the trivial ones, among which only $K^{H_0}, K^{H_1}, K^{H_3}, K^{H_7}, K^{H_8}, K^{H_9}$ are Galois extensions over $\mathbb{Q}$. And there are exact 3 subfields of degree 2 over $\mathbb{Q}$, 5 subfields of degree 4 over $\mathbb{Q}$.





$$\begin{aligned} &K^{H_1} = \mathbb{Q}(\sqrt{-1}),\ K^{H_2} = \mathbb{Q}(\alpha i),\ K^{H_3} = \mathbb{Q}(\sqrt{2}, \sqrt{-1}),\ K^{H_4} = \mathbb{Q}((1+i)\alpha), \\ &K^{H_5} = \mathbb{Q}(i\alpha),\ K^{H_6} = \mathbb{Q}((1-i)\alpha),\ K^{H_7} = \mathbb{Q}(\sqrt{2}),\ K^{H_8} = \mathbb{Q}(\sqrt{-2}). \end{aligned}$$

Exercises

1. Let $\sigma \in \mathrm{Aut}(K)$ and L a subfield of K. Show that $\sigma(L)$ is a subfield of K and $\mathrm{Gal}(K/\sigma(L)) = \sigma\mathrm{Gal}(K/L)\sigma^{-1}$.

2. Let K/F be a finite extension. Show that K/F is a Galois extension if and only if $F = K^H$ for some finite subgroup H of $\mathrm{Aut}(K)$.

3. Let $f(x)$ be a polynomial over $\mathbb{Q}$ such that $\deg f(x) = 4$ and $G_f \cong S_4$ (for example, $f(x) = x^4 - 10x^3 - 10x^2 - x - 25$). Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be all roots of $f(x)$ and $\beta = \alpha_1\alpha_2 + \alpha_3\alpha_4$. Determine the structure of $\mathrm{Gal}\left(\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)/\mathbb{Q}(\beta)\right)$.

4. Let K/F be a finite Galois extension and E/F an arbitrary extension. Assume that E and K are both contained in a common field, so that it is sensible to consider the compositum EK.

   (a) Show that EK/E is a finite Galois extension.

   (b) Show that $\mathrm{Gal}(EK/E)$ can be embedded in $\mathrm{Gal}(K/F)$, where the embedding is accomplished by restricting automorphisms in $\mathrm{Gal}(EK/E)$ to K. Furthermore, the embedding is an isomorphism if and only if $E \cap K = F$.

5. Let K be a splitting field of the polynomial $f(x) = (x^2 - 2)(x^4 - 2)$. Determine all intermediate fields of the extension $K/\mathbb{Q}$.

6. Describe all subfields of $\mathbb{Q}(\zeta_{25})$ and explicitly discuss their inclusion relation.

7. Let g be a primitive element modulo an odd prime p and $t \mid p-1$. Assume $s = \frac{p-1}{t}$. Show that $L = \mathbb{Q}(\zeta_p + \zeta_p^{g^t} + \zeta_p^{g^{2t}} + \cdots + \zeta_p^{g^{(s-1)t}})$ is Galois over $\mathbb{Q}$ and determine $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/L)$.

8. Let p be an odd prime. Determine all subfield of $\mathbb{Q}(\zeta_p)$.

9. Let K/F be a finite extension that is not necessarily Galois. Do you have any idea to find out all intermediate subfields of K/F?

10. Let
$$K = \bigcup_{n \geq 0} \mathbb{Q}(\zeta_n).$$
Show that $K/\mathbb{Q}$ is an infinite Galois extension. Do you have any idea on the Galois theory for $K/\mathbb{Q}$?

11. Suppose that $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K$, where K/F is a finite Galois extension, and that the intermediate field K_i corresponds to the subgroup H_i under the Galois correspondence. Show that K_i/K_{i-1} is Galois if and only if $H_i \lhd H_{i-1}$, and in this case, $\mathrm{Gal}(K_i/K_{i-1}) \cong H_{i-1}/H_i$.

12. Let K/F be a finite separable extension and N the normal closure of K over F in some algebraic closure.

   (a) Show that N/F is a Galois extension.

   (b) Let $G = \mathrm{Gal}(N/F)$ and $H = \mathrm{Gal}(N/K)$. Assume H' is a normal subgroup of G and $H' \subseteq H$. Show that the fixed field of H' is N. Deduce that
$$\bigcap_{g \in G} gHg^{-1} = \{1\}.$$

13. Let K/F be a finite separable extension. Show that there are finitely many intermediate subfields between F and K.

14. Let K be a finite Galois extension of F of characteristic different from 2. Suppose $\mathrm{Gal}(K/F)$ is a non-cyclic group of order 4. Show that $K = F(\alpha, \beta)$ for some $\alpha, \beta \in K$ with $\alpha^2 \in F$ and $\beta^2 \in F$.

15. Let K be the Galois closure of a finite extension $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. If p is a prime dividing the order of $\mathrm{Gal}(K/\mathbb{Q})$, show that there is a subfield F of K with $[K : F] = p$ and $K = F(\alpha)$.

2 Lecture 29 (Dec 14, 2023): Solvable Groups and Solvable by Radicals

2.1 Definition of A Solvable Group

The concept of a solvable group was introduced into mathematics by Evariste Galois, in order to state and prove his fundamental general theorems concerning the solvability of polynomial equations. We now investigate the basic properties of such solvable groups.

Definition 2.1. *A group G is said to be* **solvable** *(or soluble)* (可解的) *if there exists a finite sequence*

$$G_0 = \{1\} \subseteq G_1 \subseteq \cdots \subseteq G_{n-1} \subseteq G_n = G$$

of subgroups of G such that G_{i-1} is normal in G_i and G_i/G_{i-1} is abelian for $i = 1, 2, \ldots, n$.

The quotient group G_i/G_{i-1} in the definition is called a *group of factor* (因子群) of G.

Example 2.1. Every finite abelian group is solvable. Every non-abelian finite simple group is unsolvable.

Example 2.2. A noncommutative simple group is not solvable.

Example 2.3. The dihedral group (二面体群) D_4 of order 8, the Galois group of $x^4 - 2$ over $\mathbb{Q}$, is solvable. In fact,

$$D_4 = \langle \sigma, \tau \mid o(\sigma) = 4, o(\tau) = 2, \tau\sigma\tau = \sigma^{-1} \rangle.$$

And the sequence

$$G_0 = \{1\} \lhd G_1 = \langle \sigma \rangle \lhd G_2 = D_4$$

satisfies

$$G_1 \cong G_1/G_0 \cong \mathbb{Z}/4\mathbb{Z}, \ G_2/G_1 \cong \mathbb{Z}/2\mathbb{Z}.$$

We have another longer sequence

$$H_0 = \{1\} \lhd H_1 = \langle \sigma^2 \rangle \lhd H_2 = \langle \sigma \rangle \lhd H_3 = D_4$$

satisfies

$$H_1 \cong H_2/H_1 \cong H_3/H_2 \cong \mathbb{Z}/2\mathbb{Z}.$$

Example 2.4. The symmetries (transformation) of a rectangle that is not a square constitute a group of order 4. This group consists of the identity transformation, reflection in the axis of symmetry joining the midpoints of the two shorter sides, reflection in the axis of symmetry joining the two longer sides, and rotation though an angle of π radians (180°). If "1" denotes the identity transformation, σ and τ denote the reflections in the two axes of symmetry, and ρ denotes the rotation through π radians then $\sigma^2 = \tau^2 = \rho^2 = 1$, $\rho = \sigma\tau = \tau\sigma$, $\sigma\rho = \rho\sigma = \tau$ and $\tau\rho = \rho\tau = \sigma$. This group, denoted by V_4, is abelian:

it is often referred to as the *Klein 4-group* (or, in German, *Kleinsche Viergruppe*) (Klein 四元素群). The map

$$\begin{aligned} V_4 &\to \{1, (12)(34), (13)(24), (14)(23)\} \\ 1 &\mapsto 1 \\ \sigma &\mapsto (14)(23) \\ \tau &\mapsto (12)(34) \\ \rho &\mapsto (13)(24) \end{aligned}$$

is an isomorphism of groups from V_4 to $\{1, (12)(34), (13)(24), (14)(23)\}$. We may write the Klein 4-group

$$V_4 = \{1, (12)(34), (13)(24), (14)(23)\} \subset S_4.$$

Now we claim that the symmetric group S_4 is solvable. Indeed, let A_4 be the alternating group consisting of all even permutations of $\{1, 2, 3, 4\}$. Then $1 \lhd V_4 \lhd A_4 \lhd S_4$, V_4 is abelian, A_4/V_4 is cyclic of order 3, and S_4/A_4 is cyclic of order 2.

2.2 Solvable Groups

The concept of a solvable group was introduced into mathematics by Evariste Galois, in order to state and prove his fundamental general theorems concerning the solvability of polynomial equations. We now investigate the basic properties of such solvable groups.

Definition 2.2. *A group G is said to be* **solvable** *(or soluble)* (可解的) *if there exists a finite sequence*

$$G_0 = \{1\} \subseteq G_1 \subseteq \cdots \subseteq G_{n-1} \subseteq G_n = G$$

of subgroups of G such that G_{i-1} is normal in G_i and G_i/G_{i-1} is abelian for $i = 1, 2, \ldots, n$.

The quotient group G_i/G_{i-1} in the definition is called a *group of factor* (因子群) of G.

Example 2.5. Every finite abelian group is solvable.

Example 2.6. Every non-abelian finite simple group is unsolvable. In other words, a noncommutative solvable group can not be simple. This means a noncommutative simple group is not solvable.

Example 2.7. The dihedral group (二面体群) D_4 of order 8, the Galois group of $x^4 - 2$ over $\mathbb{Q}$, is solvable. In fact,

$$D_4 = \langle \sigma, \tau \mid o(\sigma) = 4, o(\tau) = 2, \tau\sigma\tau = \sigma^{-1} \rangle.$$

And the sequence

$$G_0 = \{1\} \lhd G_1 = \langle \sigma \rangle \lhd G_2 = D_4$$

satisfies

$$G_1 \cong G_1/G_0 \cong \mathbb{Z}/4\mathbb{Z}, \ G_2/G_1 \cong \mathbb{Z}/2\mathbb{Z}.$$

We have another longer sequence

$$H_0 = \{1\} \lhd H_1 = \langle \sigma^2 \rangle \lhd H_2 = \langle \sigma \rangle \lhd H_3 = D_4$$

satisfies

$$H_1 \cong H_2/H_1 \cong H_3/H_2 \cong \mathbb{Z}/2\mathbb{Z}.$$

Example 2.8. The symmetries (transformation) of a rectangle that is not a square constitute a group of order 4. This group consists of the identity transformation, reflection in the axis of symmetry joining the midpoints of the two shorter sides, reflection in the axis of symmetry joining the two longer sides, and rotation though an angle of π radians (180°). If "1" denotes the identity transformation, σ and τ denote the reflections in the two axes of symmetry, and ρ denotes the rotation through π radians then $\sigma^2 = \tau^2 = \rho^2 = 1$, $\rho = \sigma\tau = \tau\sigma$, $\sigma\rho = \rho\sigma = \tau$ and $\tau\rho = \rho\tau = \sigma$. This group, denoted by V_4, is abelian: it is often referred to as the *Klein 4-group* (or, in German, *Kleinsche Viergruppe*) (Klein 四元素群). The map

$$\begin{aligned} V_4 &\to \{1, (12)(34), (13)(24), (14)(23)\} \\ 1 &\mapsto 1 \\ \sigma &\mapsto (14)(23) \\ \tau &\mapsto (12)(34) \\ \rho &\mapsto (13)(24) \end{aligned}$$

is an isomorphism of groups from V_4 to $\{1, (12)(34), (13)(24), (14)(23)\}$. We may write the Klein 4-group

$$V_4 = \{1, (12)(34), (13)(24), (14)(23)\} \subset S_4.$$

Now we claim that the symmetric group S_4 is solvable. Indeed, let A_4 be the alternating group consisting of all even permutations of $\{1, 2, 3, 4\}$. Then $1 \lhd V_4 \lhd A_4 \lhd S_4$, V_4 is abelian, A_4/V_4 is cyclic of order 3, and S_4/A_4 is cyclic of order 2.

Remark 2.1. *Burnside Theorem* (1904) states that if G is a finite group of order $p^m q^n$, where p and q are prime numbers, and m and n are non-negative integers, then G is solvable. The celebrated *Feit-Thompson Theorem* (1963) states that every finite group of odd order is solvable (Feit, Walter; Thompson, John G., *Solvability of groups of odd order*, Pacific Journal of Mathematics, 13 (1963): 775-1029). In particular this implies that if a finite group is simple, it is either a prime cyclic or of even order.

John G. Thompson is a Fields Medalist of 1970.

Remark 2.2. A simple group is a group without normal subgroups different from the trivial subgroup and the whole group. The finite simple groups are the smallest "building blocks" from which one can "construct" any finite group by means of extensions. Every factor of a composition sequence of a finite group is a finite simple group, while a minimal normal subgroup is a direct product of finite simple groups. The cyclic groups of prime order are the easiest examples of finite simple groups. Only these finite simple groups occur as factors of composition sequences of solvable groups. All other finite simple groups are non-solvable, and their orders are even (Burnside Theorem).

The Classification Theorem of Finite Simple Groups states that finite simple groups can be classified completely into these five types: cyclic groups of prime group order; alternating groups of degree at least five; Lie-type Chevalley groups, Lie-type twisted Chevalley groups or the Tits group; the sporadic groups.

Although, as of 1990, some parts of the full proof of the Classification Theorem have not yet appeared in official journals, the classification of finite simple groups has been commonly accepted ever since 1982.

For $g_1, g_2 \in G$, then element $g_1^{-1} g_2^{-1} g_1 g_2$ is called the **commutator** (换位子) of g_1 and g_2. Denote $[g_1, g_2] = g_1^{-1} g_2^{-1} g_1 g_2$. Note that

$$g_1 g_2 = g_2 g_1 \cdot [g_1, g_2].$$

So $[g_1, g_2]$ measures the departure from commutativity of the elements g_1 and g_2. The set of commutators do not necessarily form a subgroup of G. We define the **commutator subgroup** (or derived subgroup)

(换位子群, 导出子群) G' (or $[G,G]$) to be the subgroup of G generated by all commutators:

$$G' = \langle [g_1, g_2] \mid g_1, g_2 \in G \rangle.$$

Since $[g_1, g_2]^{-1} = [g_2, g_1]$, it's obvious that G' coincides with the set of products of the form

$$[g_1, h_1][g_2, h_2] \cdots [g_k, h_k],\ g_i, h_i \in G.$$

The commutator group can be used to justify the commutativity of a group.

- G is abelian $\iff G' = 1$.
- For $H \lhd G$, G/H is abelian $\iff [g_1, g_2] \in H$ for all $g_1, g_2 \in G$
  $\iff G' \subseteq H$.

Theorem 2.1. *Every subgroup and homomorphic image of a solvable group are solvable.*

Proof. Assume G is solvable and $H < G$. Then there exists a series of subgroups

$$G_0 = \{1\} \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$$

such that the factor groups G_i/G_{i-1} are abelian for $i = 1, 2, \ldots, n$. Clearly $G_{i-1} \cap H \lhd G_i \cap H$. Since G_i/G_{i-1} is abelian, for $g_1, g_2 \in G_i \cap H$, $g_1^{-1}g_2^{-1}g_1g_2 \in G_{i-1}$, hence $g_1^{-1}g_2^{-1}g_1g_2 \in G_{i-1} \cap H$. So we have a sequence of subgroups

$$H_0 = \{1\} \lhd H_1 \lhd \cdots \lhd H_{n-1} \lhd H_n,$$

where $H_i = G_i \cap H$ and H_i/H_{i-1} are abelian for $i = 1, 2, \ldots, n$.

By the fundamental theorem of homomorphism, a homomorphic image of G must be isomorphic to G/H for some $H \lhd G$. Every sequence of subgroups of G, say,

$$G_0 = \{1\} \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G,$$

naturally induces a sequence of subgroups of $\overline{G} = G/H$:

$$\overline{G}_0 = \{1\} \lhd \overline{G}_1 \lhd \cdots \lhd \overline{G}_{n-1} \lhd \overline{G}_n = \overline{G},$$

where $\overline{G}_i = G_iH/H$, $i = 0, 1, \ldots, n$. It's easy to see

$$\overline{G}_i = G_iH/H = \{\overline{g} = gH \mid g \in G_i\}.$$

If G is solvable, we have a sequence of subgroups as above such that G_i/G_{i-1} is abelian. Hence $g_1^{-1}g_2^{-1}g_1g_2 \in G_{i-1}$ for all $g_1, g_2 \in G_i$. Consequently $\overline{g}_1^{-1}\overline{g}_2^{-1}\overline{g}_1\overline{g}_2 = \overline{g_1^{-1}g_2^{-1}g_1g_2} \in \overline{G}_{i-1}$. This implies that the quotient group $\overline{G}$ is solvable if G is solvable. □

The following theorem describe the inverse of the above result and provides a method to justify the solublity of a group.

Theorem 2.2. *If there exists a normal subgroup H of G such that H and G/H are solvable, then G is solvable.*

Proof. Let $H \lhd G$ and assume H and G/H are solvable. Then there exists a sequence of subgroups of $\overline{G} = G/H$

$$\overline{G}_0 = \{1\} \lhd \overline{G}_1 \lhd \cdots \lhd \overline{G}_{n-1} \lhd \overline{G}_n = \overline{G},$$

such that the factor groups $\overline{G}_i/\overline{G}_{i-1}$ are abelian for $i = 1, 2, \ldots, n$ and there exists a sequence of subgroups of H

$$H_0 = \{1\} \lhd H_1 \lhd \cdots \lhd H_{m-1} \lhd H_m = H,$$

each factor group H_j/H_{j-1} is abelian. Since $\overline{G}_{i-1} \lhd \overline{G}_i$ for $i = 0, 1, \ldots, n$, we can find subgroups $H_{m+i} < G$ so that

$$H_{m+i}/H = \overline{G}_i \text{ and } H = H_m \lhd H_{m+1} \lhd \cdots \lhd H_{m+n} \lhd H_{m+n}$$

(see Theorem 1 on page 60 in the textbook). Now each

$$H_{m+i}/H_{m+i-1} \cong H_{m+i}/H \Big/ H_{m+i-1}/H = \overline{G}_i/\overline{G}_{i-1}$$

is abelian. Thus we obtain a sequence of subgroups of G:

$$H_0 = \{1\} \lhd H_1 \lhd \cdots \lhd H_m \lhd H_{m+1} \lhd \cdots \lhd H_{m+n},$$

each factor group H_i/H_{i-1} is abelian for $i = 1, 2, \ldots, m+n$. So G is solvable. □

The alternating group A_5 is simple.

The definition of solvable groups ensures that any simple solvable group is abelian, hence cyclic. Since A_5 is simple and noncommutative, then A_5 is not solvable. If $n \geq 5$, the symmetric group S_n of all permutations of a set of n elements contains a subgroup isomorphic to A_5 (in other words, A_5 can be embedded in S_n for $n \geq 5$). Moreover any subgroup of a solvable group is solvable (Theorem 2.1). It follows therefore that

Corollary 2.1. *The symmetric group S_n is not solvable when $n \geq 5$.*

S_n is solvable only for $n = 1, 2, 3, 4$.

By the structure theorem on finite abelian groups, every finite abelian group has a sequence of subgroups such that each factor group is cyclic of prime order. A sequence of subgroups of a finite abelian group can be refined to a sequence whose factor groups are cyclic of prime order.

Theorem 2.3. *A finite group G is solvable if and only if there exists a descending sequence of subgroups*

$$G = G_n \rhd G_{n-1} \rhd \cdots \rhd G_1 \rhd G_0 = \{1\}$$

such that the factor groups G_i/G_{i-1} are cyclic of prime orders for $i = 1, 2, \ldots, n$. Furthermore, the length of a descending sequence is uniquely determined by G.

Exercises

1. Let G be a finite abelian group. Show that there exists a descending sequence of subgroups

$$G = G_n \supseteq G_{n-1} \supseteq \cdots \supseteq G_0 = \{1\}$$

such that G_{i+1}/G_i is cyclic of prime order for $i = 0, 1, \ldots, n-1$.

2. Show that S_4 is a solvable group and find a descending sequence of subgroups so that the factor groups are of prime orders.

3. Let G be a group and let H, G_1, G_2 be subgroups of G with $G_1 \lhd G_2$.

   (a) Show that $G_1 \cap H \lhd G_1 \cap H$ and $(G_2 \cap H)/(G_1 \cap H) \cong G_1(G_2 \cap H)/G_1 \hookrightarrow G_2/G_1$.

   (b) Assume $H \lhd G$. Show that $G_1H/H \lhd G_2H/H$.

4. Let x, y, z be elements in a group G. Define $x^y = y^{-1}xy$ and $[x, y, z] = [[x, y], z]$. Then

   (1) $[x, y] = [y, x]^{-1}$;

   (2) $[xy, z] = [x, z]^y[y, z], [x, yz] = [x, z][x, y]^z$;

   (3) $\left[x, y^{-1}\right] = \left([x, y]^{y^{-1}}\right)^{-1}, \left[x^{-1}, y\right] = \left([x, y]^{x^{-1}}\right)^{-1}$;

   (4) (Hall-Witt) $\left[x, y^{-1}, z\right]^y \left[y, z^{-1}, x\right]^z \left[z, x^{-1}, y\right]^x = 1$.

5. Let G be a group and $G' = [G, G]$ the commutator subgroup of G.

   (a) Show that $G' \lhd G$ and G/G' is abelian.

   (b) Let $H \lhd G$. Show that G/H is abelian if and only if $G' \subseteq H$.

6. Let $\eta : G_1 \to G_2$ be a homomorphism of groups. If G_2 is an abelian group, then $G_1' \subseteq \ker \eta$.

7. For a group G, we set $G^{(1)} = G'$ to be its commutator group. For $n \geq 2$, we define $G^{(n)} = \left(G^{(n-1)}\right)'$ to be the commutator group of $G^{(n-1)}$ inductively. Show that G is solvable if and only if $G^{(n)} = 1$ for some n.

8. Let p be a prime. Recall that a p-group is a finite group with p power elements. Show that

   (a) the center of a p-group is nontrivial;

   (b) every p-group is solvable.

9. Assume Burnside's Theorem on solvable groups. Show that each non-abelian finite simple group has order divisible by at least three distinct primes.

2.3 Solvable by Radicals

The well-known procedure for locating the roots of a quadratic polynomial with real or complex coefficients generalizes to quadratic polynomials with coefficients in a field F whose characteristic does not equal 2. Given a monic quadratic polynomial $x^2 + ax + b$ with coefficients a and b belonging to some such field F. Its roots are given by

$$\frac{-b}{2} \pm \frac{\sqrt{a^2 - 4b}}{2}. \tag{1}$$

(note that $\delta^2 \in F$)

Consider a cubic polynomial $f(x) = x^3 + ax^2 + bx + c$, where the coefficients a, b and c belong to some field F of characteristic different from 3. Then $f(x - \frac{1}{3}a) = x^3 - px - q$, where $p = \frac{1}{3}a^2 - b, q = \frac{1}{3}ab - \frac{2}{27}a^3 - c$. It suffices to restrict our attention to cubic polynomials of the form $x^3 - px - q$, where $p, q \in F$. We come to find a formula to the roots of $x^3 - px - q = 0$.

Let $f(x) = x^3 - px - q$. Then

$$f(u + v) = u^3 + v^3 + (3uv - p)(u + v) - q.$$

So we can take some elements u, v in a splitting field of $f(x)$ over F so that $3uv = p$ and $u \neq 0$. Then $f(u+v) = u^3 + \frac{p^3}{27u^3} - q$. Thus $f(u + \frac{p}{3u}) = 0$ if and only if u^3 is a root of the quadratic polynomial $x^2 - qx + \frac{p^3}{27}$. Now the roots of this quadratic polynomial are

$$\frac{q}{2} \pm \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}$$

and the product of these roots is $\frac{p^3}{27}$. Thus if one of these roots is equal to u^3 then the other is equal to v^3, where $v = \frac{p}{3u}$. It follows that the roots of the cubic polynomial $f(x) = x^3 - px - q$ are

$$\sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}}, \tag{2}$$

where the two cube roots must be chosen so as to ensure that their product is equal to $\frac{p}{3}$. This is the so called *Tartaglia-Cardano formula*. More precise, if we fixed ε and ξ so that

$$\varepsilon^2 = \frac{q^2}{4} - \frac{p^3}{27}, \quad \xi^3 = \frac{q}{2} + \varepsilon,$$

then the three roots of $f(x) = x^3 - px - q$ are described as

$$\alpha = \xi + \frac{p}{3\xi}, \ \beta = \omega\xi + \omega^2\frac{p}{3\xi}, \ \gamma = \omega^2\xi + \omega\frac{p}{3\xi}, \tag{3}$$

where ω is a 3rd primitive root of unity.

Remark 2.3. The solution to the cubic (as well as the quartic) was published by Gerolamo Cardano (1501-1576) in his treatise *Ars Magna*. However, Cardano was not the original discoverer of either of these results. The hint for the cubic had been provided by Niccolò Tartaglia, while the quartic had been solved by Ludovico Ferrari. However, Tartaglia himself had probably caught wind of the solution from another source. The solution was apparently first arrived at by a little-remembered professor of mathematics at the University of Bologna by the name of Scipione del Ferro (1465-1526). While del Ferro did not publish his solution, he disclosed it to his student Antonio Maria Fior. This is apparently where Tartaglia learned of the solution around 1541.

We now consider how to locate the roots of a quartic polynomial with coefficients in a field F of characteristic zero. A substitution of the form $x \mapsto x - c$, where $c \in F$, will reduce the problem to that of locating the roots α, β, γ and δ of a quartic polynomial f of the form $f(x) = x^4 - px^2 - qx - r$ in some splitting field L.

Now the roots α, β, γ and δ of the quartic polynomial

$$x^4 - px^2 - qx - r$$

must satisfy the equation

$$x^4 - px^2 - qx - r = (x-\alpha)(x-\beta)(x-\gamma)(x-\delta).$$

Equating coefficients of x, we find that

$$\alpha + \beta + \gamma + \delta = 0 \tag{4}$$

and

$$\begin{aligned} p &= -(\alpha\beta + \alpha\gamma + \alpha\delta + \beta\gamma + \beta\delta + \gamma\delta), \\ q &= \beta\gamma\delta + \alpha\gamma\delta + \alpha\beta\delta + \alpha\beta\gamma, \\ r &= -\alpha\beta\gamma\delta. \end{aligned}$$

Let

$$\begin{aligned}\lambda =&(\alpha+\beta)(\gamma+\delta) = -(\alpha+\beta)^2 = -(\gamma+\delta)^2,\\ \mu =&(\alpha+\gamma)(\beta+\delta) = -(\alpha+\gamma)^2 = -(\beta+\delta)^2,\\ \nu =&(\alpha+\delta)(\beta+\gamma) = -(\alpha+\delta)^2 = -(\beta+\gamma)^2.\end{aligned} \tag{5}$$

We shall show that $\lambda+\mu+\nu, \mu\nu+\lambda\nu+\lambda\mu$ and $\lambda\mu\nu$ can all be expressed in terms of p, q and r.

To do this we eliminate α from the above expressions using the identity $\alpha+\beta+\gamma+\delta = 0$. We find

$$\begin{aligned}p =&(\beta+\gamma+\delta)^2 - \gamma\delta - \beta\delta - \beta\gamma\\ =&\beta^2+\gamma^2+\delta^2+\gamma\delta+\beta\delta+\beta\gamma\\ q =&\beta\gamma\delta - (\beta+\gamma+\delta)(\gamma\delta+\beta\delta+\beta\gamma),\\ =&-(\beta^2\gamma+\beta^2\delta+\gamma^2\beta+\gamma^2\delta+\delta^2\beta+\delta^2\gamma) - 2\beta\gamma\delta,\\ r =&\beta^2\gamma\delta+\gamma^2\beta\delta+\delta^2\beta\gamma.\end{aligned}$$

Then

$$\begin{aligned}\lambda+\mu+\nu =&-\left((\gamma+\delta)^2+(\beta+\delta)^2+(\beta+\gamma)^2\right)\\ =&-2\left(\beta^2+\gamma^2+\delta^2+\gamma\delta+\beta\delta+\beta\gamma\right)\\ =&-2p,\\ \lambda^2+\mu^2+\nu^2 =&(\gamma+\delta)^4+(\beta+\delta)^4+(\beta+\gamma)^4\\ =&2(\beta^4+\gamma^4+\delta^4)+4(\beta^3\gamma+\gamma^3\delta+\gamma^3\beta+\gamma^3\delta\delta^3\beta+\delta^3\gamma)\\ &+6(\gamma^2\delta^2+\beta^2\delta^2+\beta^2\gamma^2)\\ p^2 =&\beta^4+\gamma^4+\delta^4+3(\gamma^2\delta^2+\beta^2\delta^2+\beta^2\gamma^2)\\ &+4(\beta^2\gamma\delta+\gamma^2\beta\delta+\delta^2\beta\gamma)+2(\beta^3\gamma+\beta^3\delta+\gamma^3\beta+\gamma^3\delta+\delta^3\beta+\delta^3\gamma).\end{aligned}$$

Thus

$$\begin{aligned}\lambda^2+\mu^2+\nu^2 =&2p^2-8(\beta^2\gamma\delta+\gamma^2\beta\delta+\delta^2\beta\gamma)\\ =&2p^2-8r.\end{aligned}$$

But

$$4p^2 = (\lambda+\mu+\nu)^2 = \lambda^2+\mu^2+\nu^2+2(\lambda\mu+\lambda\nu+\mu\nu).$$

Therefore

$$\lambda\mu+\lambda\nu+\mu\nu = 2p^2 - \frac{1}{2}(\lambda^2+\mu^2+\nu^2) = p^2+4r.$$

Now

$$\begin{aligned}&(\gamma+\delta)(\beta+\delta)(\beta+\gamma) = \beta^2\gamma+\beta^2\delta+\gamma^2\beta+\gamma^2\delta+\delta^2\beta+\delta^2\gamma+2\beta\gamma\delta = -q,\\ &(\alpha+\beta)(\alpha+\gamma)(\alpha+\delta) = -(\gamma+\delta)(\beta+\delta)(\beta+\gamma) = q\end{aligned}$$

and note that

$$\lambda\mu\nu = -\left((\gamma+\delta)(\beta+\delta)(\beta+\gamma)\right)^2.$$

Therefore

$$\lambda\mu\nu = -(-p)^2 = -q^2. \tag{6}$$

Thus λ, μ and ν are the roots of the resolvent cubic

$$x^3+2px^2+(p^2+4r)x+q^2. \tag{7}$$

With the help of (4) and (5), one can then verify that the roots of f take the form $\frac{1}{2}(\sqrt{-\lambda}+\sqrt{-\mu}+\sqrt{-\nu})$, where these square roots are chosen to ensure that $\sqrt{-\lambda}\sqrt{-\mu}\sqrt{-\nu} = q$. (It should be noted that there are four possible ways in which the square roots can be chosen to satisfy this condition; these yield

all four roots of the polynomial f.) We can therefore determine the roots of f in an appropriate splitting field once we have expressed the quantities λ, μ and ν in terms of the coefficients of the polynomial:

$$\begin{aligned}
\alpha &= \frac{1}{2}(\sqrt{-\lambda} - \sqrt{-\mu} + \sqrt{-\nu}), \\
\beta &= \frac{1}{2}(\sqrt{-\lambda} + \sqrt{-\mu} - \sqrt{-\nu}), \\
\gamma &= \frac{1}{2}(-\sqrt{-\lambda} + \sqrt{-\mu} + \sqrt{-\nu}), \\
\delta &= \frac{1}{2}(-\sqrt{-\lambda} - \sqrt{-\mu} - \sqrt{-\nu}).
\end{aligned} \tag{8}$$

Is there a formula for the roots of a quintic polynomial? What's the exact meaning of "formula" for the roots of a polynomial?

Definition 2.3. *Let F be a field. A polynomial $f(x) \in F[x]$ is* **solvable by radicals** (可根式求解) *if the roots of the polynomial in a splitting field can be constructed from its coefficients in a finite number of steps involving only the operations of addition $(+)$, subtraction $(-)$, multiplication $(\times)$, division $(\div)$ and extraction of n-th roots for appropriate positive numbers n ($\sqrt[n]{\ }$).*

By the above discussion, we have

Proposition 2.1. *Let $f(x)$ be a polynomial of degree ≤ 4 over a field of characteristic 0. Then $f(x)$ is solvable by radicals.*

It follows from Definition 2.3 that a polynomial $f(x) \in F[x]$ is solvable by radicals if and only if there exist fields $F_0, F_1, \ldots, F_n$ such that $F_0 = F$, the polynomial f splits over F_n, and, for each integer i between 1 and n, the field $F_i = F_{i-1}(\alpha_i)$, where $\alpha_i^{m_i} \in F_{i-1}$ for some positive integer m_i. Hence

Proposition 2.2. *A polynomial $f(x) \in F[x]$ is solvable by radicals if and only if there exists a tower of fields*

$$F_0 = F \subseteq F_1 \subseteq \cdots \subseteq F_n$$

such that

1. *$f(x)$ splits over F_n;*
2. *$F_i = F_{i-1}(\sqrt[m_i]{a_i})$, where $\sqrt[m_i]{a_i}$ denotes a root of the polynomial $x^{m_i} - a_i$ for some $a_i \in F_{i-1}$ and positive integer $m_i \in \mathbb{Z}$, $i = 1, 2, \ldots, n$.*

In other words, a polynomial $f(x) \in F[x]$ is solvable by radicals if and only if $f(x)$ splits in an extension field K such that $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$, where $\alpha_1^{m_1} \in F$ and $\alpha_i^{m_i} \in F(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$ for some $m_i \in \mathbb{Z}$ and for each $i = 2, 3, \ldots, n$.

An extension of the form $F(\alpha)/F$, where $\alpha^n \in F$ for some $n \in \mathbb{Z}$, is called a **single radical extension** (单根式扩张). In other words, a single radical extension is a simple extension of the form $F(\sqrt[n]{a})$ for some positive integer n and $a \in F$. In particular, if α is a root of unity, then then $F(\alpha)/F$ is called a *cyclotomic extension* (分圆扩张).

The field extension F_n/F_0 as in Proposition 2.2 is called a radical extension. The extension E/F is called **radical** (根式扩张), if there exist a series of intermediate fields E_i such that

$$F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = E$$

and E_i/E_{i-1} is a single radical extension for $1 \le i \le n$. Hence a radical extension is realized by a successive single radical extensions.

We explain Proposition 2.2 for polynomials of degree 2 and 3. For quadratic polynomial x^2+ax+b, its roots are given by (1). We may adjoin to F an element δ satisfying $\delta^2 = a^2 - 4b \in F$. Then all roots are contained in $F_1 = F(\delta)$, a radical extension over F.

For a cubic polynomial $x^3 - px - q \in F[x]$, its roots are given by (3). Hence

$$F \subseteq F(\varepsilon) \subseteq F(\varepsilon, \xi) \subseteq F(\varepsilon, \xi, \omega)$$

and

$$\varepsilon^2 \in F, \quad \xi^3 \in F(\varepsilon),\ \omega^3 \in F(\varepsilon, \xi).$$

And $F(\varepsilon)/F, F(\varepsilon,\xi)/F(\varepsilon), F(\varepsilon,\xi,\omega)/F(\varepsilon,\xi)$ are radical extensions. We find out all three roots are contained in the radical extension $K = F(\varepsilon, \xi, \omega)$.

For a quartic polynomial like $x^4 - px^2 - qx - r$, its root are given by formula (8). Can you find a sequence of subfields of $F(\sqrt{-\lambda}, \sqrt{-\mu}, \sqrt{-\nu})$ with the required property as we did in the cubic case?

Proposition 2.2 shows

Theorem 2.4. *A polynomial $f(x) \in F[x]$ is solvable by radicals if and only if $f(x)$ splits in some radical extension.*

A polynomial is solvable by radicals $\Longleftrightarrow$ the splitting field of the polynomial is contained in some radical extension.

We next consider the possibilities for the Galois group $\mathrm{Gal}(L/F)$, where L is a splitting field for $f(x) = x^3 - px - q$ over F. Now $L = F(\alpha, \beta, \gamma)$, where α, β and γ given in (3) are the roots of $f(x)$. A F-automorphism of L must permute the roots of $f(x)$ amongst themselves, and it is determined by its action on these roots. Therefore $\mathrm{Gal}(L/F)$ is isomorphic to a subgroup of the symmetric group S_3 (i.e., the group of permutations of a set of 3 objects), and thus the possibilities for the order of $\mathrm{Gal}(L/F)$ are 1, 2, 3 and 6. One can see that $f(x)$ is irreducible over F if and only if $|\mathrm{Gal}(L/F)| = 3$ or 6. If $f(x)$ splits over F then $|\mathrm{Gal}(L/F)| = 1$. If $f(x)$ factors in $F[x]$ as the product of a linear factor and an irreducible quadratic factor then $|\mathrm{Gal}(L/F)| = 2$.

Let $\delta = (\alpha - \beta)(\beta - \gamma)(\alpha - \gamma)$. Then δ^2 is invariant under any permutation of α, β and γ, and therefore δ^2 is fixed by all automorphisms in the Galois group $\mathrm{Gal}(L/F)$ (δ^2 is symmetric in α, β, γ). Therefore $\delta^2 \in F$. The element δ^2 of F is referred to as the discriminant of the polynomial $f(x)$. A straightforward calculation shows that if $f(x) = x^3 - px - q$ then the discriminant

$$D(f) = \delta^2 = 4p^3 - 27q^2.$$

Now δ changes sign under any permutation of the roots α, β and γ that transposes two of the roots whilst leaving the third root fixed. But $\delta \in F$ if and only if δ is fixed by all elements of the Galois group $\mathrm{Gal}(L/F)$, in which case the Galois group must induce only cyclic permutations of the roots α, β and γ. *If $f(x)$ is irreducible over F, the Galois group*

$$\mathit{Gal}(f(x)/F) \cong \begin{cases} A_3, & \text{if } D(f) \text{ is a square in } F, \\ S_3, & \text{if } D(f) \text{ is not a square in } F. \end{cases}$$

In each case, the Galois group of $x^3 - px - q$ is a solvable group, as is the reason why $x^3 - px - q$ is solvable by radicals if $\mathrm{char}\, F = 0$, due to Galois Theorem in the following lectures.

Exercises

1. Let $f(x)$ be an irreducible polynomial of degree n over $\mathbb{Q}$ with $n \geq 3$ and K the splitting field of $f(x)$. Assume $\alpha \in K$ is a root of $f(x)$ and $[K : \mathbb{Q}] = n!$. Show that $\mathbb{Q}(\alpha^4) = \mathbb{Q}(\alpha)$.

2. Let K be a radical extension of F.

   (a) Let σ be an F-embedding on K. Show that $\sigma(K)/F$ is a radical extension.

   (b) Show that the normal closure of K/F is also a radical extension over F.

3. Let F be a finite field of characteristic p. Show that if $f(x) \in F[x]$ is an irreducible polynomial and the degree of $f(x)$ is less than p, then $f(x) = 0$ is solvable by radicals.

4. Let p be a prime and let $F = \mathbb{F}_p(t)$ be the rational function field over the finite field $\mathbb{F}_p$. Let K be a splitting field of the polynomial $f(x) = x^p - x - t$ over F.

   (1) Show that the Galois group of $f(x)$ is cyclic of order p;

   (2) Show that K/F is not solvable by radicals.

5. Show that a polynomial $f(x) \in F[x]$ is solvable by radicals if $f(x)$ splits in an extension field K such that $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$, and $\alpha_i^{p_i} \in F(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$ for some prime integers p_i and for each $i = 2, 3, \ldots, n$.

2.4 Basic Facts on S_n

- For $\sigma \in S_n$, $\sigma(i_1 i_2 \cdots i_r)\sigma^{-1} = (\sigma(i_1)\,\sigma(i_2)\,\cdots\,\sigma(i_r))$.
- For the full symmetric group S_n, we have

$$\begin{aligned} S_n &= \langle (i_1 i_2 \cdots i_r) \mid 1 \leq i_1, i_2, \ldots, i_r \leq n \rangle, \\ &= \langle (i_1 i_2) \mid 1 \leq i_1 < i_2 \leq n \rangle, \\ &= \langle (1\, i) \mid 1 < i \leq n \rangle, \\ &= \langle (i, i+1) \mid 1 \leq i \leq n-1 \rangle, \\ &= \langle (12), (12 \cdots n) \rangle. \end{aligned}$$

  Since

$$\begin{aligned} &(i_1 i_2 \cdots i_r) = (i_1 i_r) \cdots (i_1 i_4)(i_1 i_3)(i_1 i_2), \\ &(i_1 i_2 \cdots i_r) = (1 i_r) \cdots (1 i_4)(1 i_3)(1 i_2) \quad \text{if} \quad i_1 = 1 \quad \text{and} \\ &(i_1 i_2 \cdots i_r) = (1\, i_2 \cdots i_r i_1)(1\, i_1) = (1\, i_1)(1 i_r) \cdots (1 i_3)(1 i_2)(1\, i_1) \quad \text{if} \quad i_1, i_2, \ldots, i_r \neq 1, \end{aligned}$$

$$\begin{aligned} (i, i+1) &= (1i)(1, i+1)(1i), \\ (1, i+1) &= (1\, i)(i, i+1)(1\, i), \\ (i, i+1) &= (12 \cdots n)^{i-1}(12)(12 \cdots n)^{1-i}. \end{aligned}$$

- The alternating group A_5 is a simple group of order 60.
- S_n is solvable for $n \leq 4$, while S_n is insolvable for $n \geq 5$.
- If p is a prime, then all elements of order p in S_p are of the form $(i_1 i_2 \cdots i_p)$, a p-cycle.
- The Galois group of a polynomial of degree n can be embedded as a subgroup of S_n.

Homework Exercise 23, 25, 26, 28, 30 on page 317-318. Exercise 25, 43, 45 on page 99-100.