

## Chapter V. Solvability by Radicals

One of the oldest problems in algebra was to find roots of an equation. Already in the antiquity solutions of quadratic equations were known. In the renaissance one knew - modulo lacking exact knowledge of complex numbers - solutions of cubic and quartic equations expressed by successive application of the four classical arithmetical operations and extractions of roots (i.e. radicals). (More details follow later in this chapter.)

For several centuries it was an open problem to "solve" (meaning solving by radicals) an equation of degree 5 or of higher degree. The first real break-through came from the Italian physician and mathematician Paolo Ruffini (1765-1822). In 1799 he published "Teoria generale delle equazioni" containing the assertion that an equation of degree 5 in general cannot be solved by taking radicals and using the four classical arithmetical operations. His "proof" contained many errors and obscurities, but the basic underlying ideas were correct. It was also something of a feat that he at all - as the first one - got the idea that such equations in general could not be solved by radicals. His work did not get much response from his contemporaries. The first recognized proof that the "general quintic equation" cannot be solved by radicals was due to the Norwegian mathematician Niels Henrik Abel (1802-29), who treated this subject in a paper ("Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré") from 1824. (However, there has been some discussion whether his proof really was quite correct.)

Only by the papers by Galois (especially "Mémoire sur les conditions de résolubilité des équations par radicaux", published many years after his death) the problem got a systematical and fully satisfactory treatment.

In this chapter we give a presentation of this, where we use modern terminology and concepts.

We first bring some abstract theorems which off-hand do not seem to have much to do with quintic equations etc.

### CROSSED PRODUCTS AND APPLICATIONS.

Let  $G$  be a group of automorphisms of a field  $K$ .

DEFINITION 5.1. A mapping  $f$  from  $G$  into  $K^*$  (the multiplicative group of the non-zero elements of  $K$ ) is called a *crossed homomorphism*, if it satisfies the condition

$$f(\sigma\tau) = \sigma(f(\tau)) \cdot f(\sigma) \quad \forall \sigma, \tau \in G.$$

Clearly  $f(e) = 1$  for every crossed homomorphism  $f$ . The product of two crossed homomorphisms is again a crossed homomorphism and in this way the crossed homomorphisms form a commutative group  $H$ .

If  $a$  is an element of  $K^*$  it is straightforward to check that the mapping from  $G$  to  $K^*$  defined by  $f(\sigma) = \frac{a}{\sigma(a)}$  is a crossed homomorphism.

A crossed homomorphism of this form is called “*principal*”. The principal crossed homomorphisms form a subgroup  $P$  of  $H$ .

DEFINITION 5.2. The factor group  $H/P$  is called *the 1’st cohomology group* for  $G$  with coefficients in  $K$  and is denoted  $H^1(G, K^*)$ .

**Theorem 5.3.** *If  $G$  is a finite group of automorphisms, then  $H^1(G, K^*) = 1$ ; in other words: every crossed homomorphism is principal.*

*Proof.* Since distinct automorphisms are independent over  $K$  (Theorem 3.15 in Chap. III) there exists an element  $x$  in  $K$  such that  $\sum_{\tau \in G} f(\tau)\tau(x) \neq 0$ , where  $f$  is an arbitrary crossed homomorphism. If we set  $a = \sum_{\tau \in G} f(\tau)\tau(x)$ , then

$$\begin{aligned} \sigma(a) &= \sum_{\tau} \sigma f(\tau)\sigma\tau(x) = \sum_{\tau} \frac{f(\sigma\tau)}{f(\sigma)} \cdot \sigma\tau(x) = \\ &= \frac{1}{f(\sigma)} \sum_{\tau} f(\tau)\tau(x) = \frac{a}{f(\sigma)}, \text{ hence } f(\sigma) = \frac{a}{\sigma(a)} \end{aligned}$$

i.e.:  $f$  is principal. □

EXAMPLE 5.4. If  $G$  is not finite,  $H^1(G, K^*)$  may be non-trivial. A counterexample is the following: Let  $K = \mathbb{C}(X)$  and  $G$  the group of automorphisms of  $K$  defined by  $\sigma\left(\frac{f(x)}{g(x)}\right) = \frac{f(x+1)}{g(x+1)}$ ,  $G = \{\sigma^n | n \in \mathbb{Z}\}$ . We define a crossed homomorphism  $f$  from  $G$  into  $K^*$  by

$$\begin{aligned} f(\sigma) &= x \\ f(\sigma^n) &= x \cdot \sigma(x) \dots \sigma^{n-1}(x) & n > 0 \\ f(\sigma^{-n}) &= \sigma^{-1}\left(\frac{1}{x}\right) \dots \sigma^{-n}\left(\frac{1}{x}\right) & n > 0. \end{aligned}$$

Then  $f$  is not principal (why?)

Before giving the first application of Theorem 5.3, we introduce the notion of norm. Let  $L/K$  be a finite normal extension. For an element  $\alpha$  in  $L$  we define the *norm*  $N_{L/K}(\alpha)$  as the product  $\prod_{\sigma \in \text{Gal}(L/K)} \sigma(\alpha)$ . (Cf. the definition of trace in Lemma 3.18 Chap. III.)

By the same argument as for traces we see that for any  $\alpha$  in  $L$  the norm  $N_{L/K}(\alpha)$  is invariant under all automorphism in  $\text{Gal}(L/K)$  and therefore lies in  $K$ . It is straightforward to check the following rules

- i)  $\alpha \neq 0$  iff  $N_{L/K}(\alpha) \neq 0$ .
- ii) The norm is multiplicative:  $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$  for any two elements  $\alpha$  and  $\beta$  in  $L$ .
- iii)  $N_{L/K}(\alpha) = N_{L/K}(\sigma(\alpha))$  for every  $\alpha \in K$  and every  $\sigma \in \text{Gal}(L/K)$ .

From i), ii) and iii) we conclude that an element  $\beta \in L$  has norm 1 if  $\beta$  can be written as  $\frac{\alpha}{\sigma(\alpha)}$  for some  $\alpha \in K \setminus 0$  and some  $\sigma \in \text{Gal}(L/K)$ .

The converse is in general not true, but for normal extensions with cyclic Galois group the following holds

**Corollary 5.5.** (“Hilbert Satz 90”) *Let  $L/K$  be a finite normal extension with cyclic Galois group  $\text{Gal}(L/K) = \{e, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$ . If  $\beta \in L$  and  $N_{L/K}(\beta) = \prod_{i=0}^{n-1} \sigma^i(\beta) = 1$ , then there exists  $\alpha \in L \setminus \{0\}$  such that  $\beta = \frac{\alpha}{\sigma(\alpha)}$ .*

*Proof.* We define a mapping  $f$  from  $\text{Gal}(L/K)$  into  $L^*$  by

$$\begin{aligned} f(e) &= 1 \\ f(\sigma) &= \beta \\ &\dots \\ f(\sigma^2) &= \beta\sigma(\beta) \\ f(\sigma^{n-1}) &= \beta\sigma(\beta) \dots \sigma^{n-2}(\beta). \end{aligned}$$

Since the product  $\beta\sigma\beta \dots \sigma^{n-2}(\beta)\sigma^{n-1}(\beta)$  by assumption is 1 it follows that  $f(\sigma^j) = \beta \cdot \sigma(\beta) \dots \sigma^{j-1}(\beta)$  for all  $j > 0$ . Therefore  $f$  is a crossed homomorphism. Indeed:

$$f(\sigma^i \sigma^j) = \beta \sigma(\beta) \dots \sigma^{i+j-1}(\beta)$$

and

$$\sigma^i f(\sigma^j) f(\sigma^i) = [\sigma^i \beta \cdot \sigma^{i+1}(\beta) \dots \sigma^{i+j+1}(\beta)] \cdot [\beta \cdot \sigma(\beta) \dots \sigma^{i-1}(\beta)].$$

By Theorem 5.3  $f$  is principal i.e.:  $\exists \alpha \in L \setminus \{0\}$  such that

$$\begin{aligned} f(\sigma^i) &= \frac{\alpha}{\sigma^i(\alpha)} \forall i, \quad \text{in particular:} \\ \beta &= f(\sigma) = \frac{\alpha}{\sigma(\alpha)}. \end{aligned}$$

□

Before bringing the most important application for our purposes of the results above we give some general theorems concerning Galois groups for binomials (i.e. polynomials of the form  $x^n - a$ ).

Let  $K$  be a field of characteristic 0 and let  $n$  be a natural number. Assume  $K$  contains the  $n$ -th roots of unity, (in other words:  $\mathbb{Q}_n \subseteq K$ ).

**Theorem 5.6.** *Under the above assumptions the following holds: If  $M$  is the splitting field for  $x^n - a$ , ( $a \in K$ ), over  $K$ , then  $M/K$  is normal and the Galois group  $\text{Gal}(M/K)$  is cyclic of an order dividing  $n$ .*

*Proof.* The case  $a = 0$  is trivial, so we may assume that  $a$  is  $\neq 0$ . If  $\varepsilon$  denotes a primitive  $n$ -th root of unity and  $\beta$  is a root of  $x^n - a$ , then all roots of  $x^n - a$  are exactly  $\beta, \beta\varepsilon, \beta\varepsilon^2, \dots, \beta\varepsilon^{n-1}$ , hence:  $x^n - a = (x - \beta)(x - \beta\varepsilon) \cdots (x - \beta\varepsilon^{n-1})$  (distinct roots). Consequently  $M = K(\beta)$ .

Let  $\sigma \in \text{Gal}(M/K)$ ,  $\sigma(\beta) = \beta \cdot \varepsilon^i$ ,  $0 \leq i < n$ . We define the mapping  $\varphi$  from  $\text{Gal}(M/K)$  into the cyclic group of  $n$ -th roots of unity by:  $\varphi(\sigma) = \frac{\beta}{\sigma(\beta)}$ .

$\sigma$  is uniquely determined by its value on  $\beta$ , hence  $\varphi$  is injective.  $\varphi$  is a homomorphism:

$$\varphi(\sigma\tau) = \frac{\beta}{\sigma\tau(\beta)} = \frac{\beta}{\sigma(\beta)} \cdot \frac{\sigma(\beta)}{\sigma\tau(\beta)} = \frac{\beta}{\sigma(\beta)} \cdot \sigma\left(\frac{\beta}{\tau(\beta)}\right).$$

$\frac{\beta}{\tau(\beta)}$  is an  $n$ -th root of unity which by assumption lies in  $K$ ; therefore  $\sigma\left(\frac{\beta}{\tau(\beta)}\right) = \frac{\beta}{\tau(\beta)}$ :

$$\varphi(\sigma\tau) = \frac{\beta}{\sigma(\beta)} \frac{\beta}{\tau(\beta)} = \varphi(\sigma)\varphi(\tau).$$

Consequently  $\text{Gal}(M/K)$  is isomorphic to a subgroup of the group of  $n$ -th roots of unity, i.e.:  $\text{Gal}(M/K)$  is cyclic and  $|\text{Gal}(M/K)|$  divides  $n$ .  $\square$

**Theorem 5.7.** *Let  $p$  be a prime number and  $K$  a field of characteristic 0 containing the  $p$ -th roots of unity. For an arbitrary  $a \in K$  the polynomial  $x^p - a$  is either irreducible in  $K[x]$  or splits into a product of linear polynomials in  $K[x]$ .*

*Proof.* We may assume  $a \neq 0$ . The splitting field  $M$  for  $x^p - a$  over  $K$  is obtained by adjoining a root  $\beta$  of  $x^p - a$ ; hence  $M = K(\beta)$ . By the previous theorem  $[M : K]$  divides  $p$ , i.e.:  $[M : K] = 1$  or  $[M : K] = p$ . If  $[M : K] = 1$  the root  $\beta$  and thereby all roots of  $x^p - a$  lie in  $K$ . In the case  $[M : K] = p$  we notice, that  $\text{Irr}(\beta, K) | x^p - a$ . Since  $\text{degree}(\text{Irr}(\beta, K)) = \text{degree}(x^p - a)$  we see that  $x^p - a = \text{Irr}(\beta, K)$ , i.e.:  $x^p - a$  is irreducible.  $\square$

The following theorem may be considered as sort of converse of Theorem 5.6.

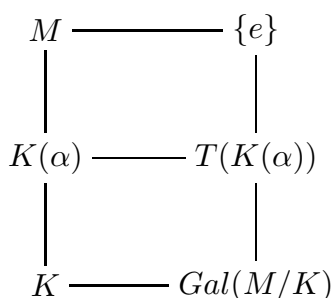
**Theorem 5.8.** *Let  $K$  be a field of characteristic 0 and  $n$  a natural number. Assume  $K$  contains all  $n$ -th roots of unity. If  $M/K$  is a finite normal extension with cyclic Galois group of order  $n$ , then  $M = K(\alpha)$  for a suitable  $\alpha \in M$ , where  $\alpha^n$  is an element in  $K$ .*

*Proof.* Let  $\text{Gal}(M/K) = \{e, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$  and let  $\varepsilon$  be a primitive  $n$ -th root of unity. By assumption  $\varepsilon$  lies in  $K$  and thus the product (norm)  $\prod_{i=0}^{n-1} \sigma^i(\varepsilon) = \varepsilon^n$  is 1.

By corollary 5.5 there exists an  $\alpha \in M$  for which  $\frac{\alpha}{\sigma(\alpha)} = \varepsilon$ . Then

$$\begin{aligned} \sigma(\alpha) &= \alpha\varepsilon^{-1} \\ \sigma^2(\alpha) &= \alpha\varepsilon^{-2} \\ &\dots \\ &\dots \\ \sigma^{n-1}(\alpha) &= \alpha\varepsilon^{-(n-1)} \end{aligned}$$

and we have diagrams for subfields of  $M$  and subgroups of  $\text{Gal}(M/K)$ :



$$\begin{aligned} TK(\alpha) &= \{\tau \in \text{Gal}(M/K) \mid \tau\alpha = \alpha\} = \{e\} \\ K(\alpha) &= \mathcal{F}(T(K(\alpha))) = \mathcal{F}(\{e\}) = M \end{aligned}$$

$\sigma(\alpha^n) = \alpha^n$  i.e.:  $\alpha^n$  belongs to  $K$ . □

EXERCISE 5.9. Let  $L = \mathbb{Q}(\sqrt[p]{2}, \varepsilon)$ , where  $p$  is an odd prime number and  $\varepsilon$  is a primitive  $p$ -th root of unity.

- 1) Find  $[L : \mathbb{Q}]$ .
- 2) Show that  $L/\mathbb{Q}$  is normal with a non-abelian Galois group.
- 3) Let  $\alpha$  be a number in  $L$ , such that  $L = \mathbb{Q}(\alpha, \varepsilon)$ , where  $\alpha^p \in \mathbb{Q}(\varepsilon)$ .

Show that  $\alpha^p = \beta^p \cdot 2^t$ ,  $1 \leq t \leq p - 1$ ,  $\beta \in \mathbb{Q}(\varepsilon)$ . (*Hint*: write  $\alpha$  as a  $\mathbb{Q}(\varepsilon)$ -linear combination of  $1, \sqrt[p]{2}, \dots, (\sqrt[p]{2})^{p-1}$  and apply the automorphism  $\sigma \in \text{Gal}(L/\mathbb{Q}(\varepsilon))$  determined by  $\sigma(\sqrt[p]{2}) = \varepsilon\sqrt[p]{2}$ ).

- 4) For which  $a \in \mathbb{Q}$  is  $L$  the splitting field (over  $\mathbb{Q}$ ) for  $x^p - a$ ?

**RADICAL EXTENSIONS.**

In the remainder of this chapter we shall only consider fields of characteristic 0. An extension  $M/K$  is called *abelian* (resp. *cyclic*), if  $M/K$  is normal with abelian (resp. cyclic) Galois group.

DEFINITION 5.10. An extension is called a *radical extension*, if there exist intermediate fields  $K_0 = K, K_1, K_2, \dots, K_t = M$  such that

$$\begin{aligned} K_1 &= K_0(\alpha_1) & \alpha_1^{n_1} &\in K_0 & \text{for a suitable natural number } n_1, \\ K_2 &= K_1(\alpha_2) & \alpha_2^{n_2} &\in K_1 & \text{for a suitable natural number } n_2, \\ & \dots\dots\dots \\ K_t &= K_{t-1}(\alpha_t) & \alpha_t^{n_t} &\in K_{t-1} & \text{for a suitable natural number } n_t. \end{aligned}$$

The motivation for the above definition is the following: When we want to say that the roots of a polynomial, say in  $\mathbb{Q}[X]$ , cannot be found by application of the four classical arithmetical operations and extractions of roots, we have to formalize such procedures. By the above definition every field  $K_i$  is obtained by adjoining a root  $\sqrt[n_i]{a_i}, (a_i = \alpha_i^{n_i} \in K_{i-1})$ . That a number lies in a radical extension where for instance  $K_0 = \mathbb{Q}$ , means exactly that it can be obtained by starting with elements (numbers) in the base field  $\mathbb{Q}$  and carrying out a finite sequence of the rational (classical) arithmetical operations and solving equations of the form  $x^n = a$ .

DEFINITION 5.11. An extension  $M/K$  is called *meta-abelian*, if there exist intermediate fields  $K_0 = K, K_1, K_2, \dots, K_t$  so that  $K_1/K_0, K_2/K_1, \dots, K_t/K_{t-1}$  are abelian.

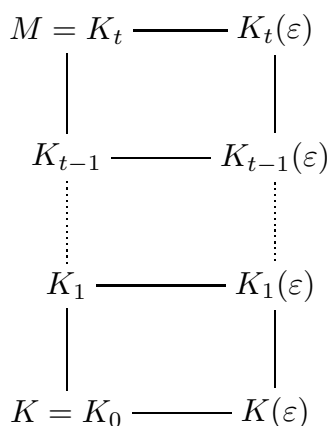
**Theorem 5.12.** *Every radical extension can be embedded in a meta-abelian extension.*

*Proof.* Let  $M/K$  be a radical extension.

Then there are  $K_1, K_2, \dots, K_t = M$  such that  $K_i = K_{i-1}(\alpha_i), \alpha_i^{n_i} \in K_{i-1}, i = 1, 2, \dots, t. (K_0 = K).$

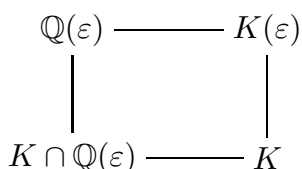
Let  $n = n_1 n_2 \dots n_t$ , and let  $\varepsilon$  be a primitive  $n$ -th root of unity.

We have the following diagrams of fields:



Clearly for each  $i$ ,  $1 \leq i \leq t$  we have  $K_i(\varepsilon) = K_{i-1}(\varepsilon)(\alpha_i)$ ,  $\alpha_i^{n_i} \in K_{i-1}(\varepsilon)$ . Now  $K_{i-1}(\varepsilon)$  contains the  $n_i$ -th roots of unity since  $n_i$  divides  $n$  and  $K_{i-1}(\varepsilon)$  contains the  $n$ -th roots of unity. Because  $K_i(\varepsilon)$  is the splitting field for  $x^{n_i} - \alpha_i^{n_i}$  over  $K_{i-1}(\varepsilon)$ , Theorem 5.6 implies that  $K_i(\varepsilon)/K_{i-1}(\varepsilon)$ ,  $i = 1, 2, \dots, t$ , is normal with cyclic Galois group.

Since the field  $K$  has characteristic 0, it contains the rational number field  $\mathbb{Q}$ . We have the following diagram:

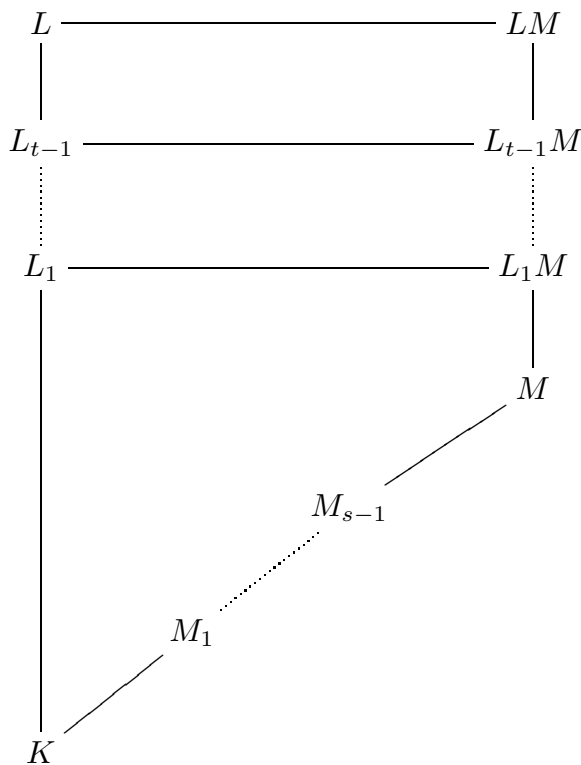


The translation theorem shows that  $K(\varepsilon)/K$  is normal with a Galois group which is isomorf to  $\text{Gal}(\mathbb{Q}(\varepsilon)/K \cap \mathbb{Q}(\varepsilon))$  i.e.:  $K(\varepsilon)/K$  is abelian.

Hence  $K_t(\varepsilon)/K$  is a meta-abelian extension of  $K$  containing  $M$ . □

**Theorem 5.13.** *Let  $L \supseteq K$  and  $M \supseteq K$  be two meta-abelian extensions contained in some common field. Then the compositum  $LM$  is a meta-abelian extension of  $K$ .*

*Proof.* Let  $L = L_t \supset L_{t-1} \supset \dots \supset L_0 = K$  and  $M = M_s \supset M_{s-1} \supset \dots \supset M_0 = K$  be intermediate fields such that  $L_i/L_{i-1}$  og  $M_j/M_{j-1}$  are abelian. We now have the following diagram:



Because of the translation theorem the extensions  $L_iM/L_{i-1}M$  are abelian; hence the above diagram shows that  $ML$  is a meta-abelian extension of  $K$ .  $\square$

**Theorem 5.14.** *Every meta-abelian extension  $L/K$  can be embedded in a normal meta-abelian extension.*

*Proof.* By Abel-Steinitz' theorem we can write  $L$  as  $K(\alpha)$ . (Since the fields in this final section have characteristic 0,  $L/K$  is a separable extension.) If  $M$  is the splitting field over  $K$  for  $f(x) = \text{Irr}(\alpha, K)$ , then  $M$  is a normal extension of  $K$  containing  $L$ . Let  $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$  be the roots of  $f(x)$ . Then  $M = K(\alpha_1, \dots, \alpha_n)$  is the compositum of the fields  $K(\alpha_1), \dots, K(\alpha_n)$ .

For each of the fields  $K(\alpha_i), 1 \leq i \leq n$ , there is (by Theorem 2.57 in Chap. II) an isomorphism of  $L = K(\alpha_1)$  onto  $K(\alpha_i)$ , which is the identity on  $K$ . Since  $L/K$  is meta-abelian, the isomorphic extensions  $K(\alpha_i)/K, 1 \leq i \leq n$ , are also meta-abelian. Theorem 5.13 implies that the compositum of these extensions is meta-abelian. But this compositum is just  $M$ , which therefore is a normal meta-abelian extension of  $K$  containing  $L$ .  $\square$

**Corollary 5.15.** *Every radical extension can be embedded in a normal meta-abelian extension.*

**Theorem 5.16. The Main Theorem about Solvability by Radicals.** *Let  $f(x)$  be an irreducible polynomial in  $K[x]$  and  $M$  its splitting field over  $K$ . The following conditions are equivalent:*

- i) There exists a radical extension of  $K$  in which  $f(x)$  has a root.*
- ii) There exists a radical extension of  $K$  in which  $f(x)$  has all its roots.*
- iii) The Galois group  $\text{Gal}(M/K)$  is solvable.*

*Proof.* 'Obviously ii) implies i). Hence it suffices to show i)  $\Rightarrow$  iii) and iii)  $\Rightarrow$  ii) .

i)  $\Rightarrow$  iii):  $f(x)$  has a root in a suitable radical extension  $L$  of  $K$ . By the Corollary there exists a normal meta-abelian extension  $\widetilde{M}$  of  $K$  such that  $\widetilde{M} \supseteq L$ . Since  $f(x)$  has a root in  $\widetilde{M}$  and  $\widetilde{M}/K$  is normal,  $f(x)$  splits into linear factors in  $\widetilde{M}$  (cf. Theorem 3.27 in Chap. III), i.e.:  $\widetilde{M} \supseteq M$ .

We now insert the following

**Lemma 5.17.** *Let  $M/K$  be a finite normal extension. Then:*

$$M/K \text{ is meta-abelian} \Leftrightarrow \text{Gal}(M/K) \text{ is solvable.}$$

*Proof of Lemma 5.17. “ $\Rightarrow$ ”*

Since  $M/K$  is meta-abelian there exist intermediate fields  $K_0 = K, K_1, \dots, K_t$ , such that  $K_1/K_0, \dots, K_t/K_{t-1}$  are abelian:

$$\begin{array}{ccc}
 M = K_t & \text{-----} & T(K_t) = \{e\} \\
 | & & | \\
 K_{t-1} & \text{-----} & T(K_{t-1}) \\
 \vdots & & \vdots \\
 K_1 & \text{-----} & T(K_1) \\
 | & & | \\
 K & \text{-----} & T(K) = Gr(M/K)
 \end{array}$$

Since  $K_i/K_{i-1}$  is abelian,  $T(K_{i-1})/T(K_i)$  is abelian, so  $Gal(M/K)$  has a normal series with abelian factors and is therefore solvable.

” $\Leftarrow$ ”:

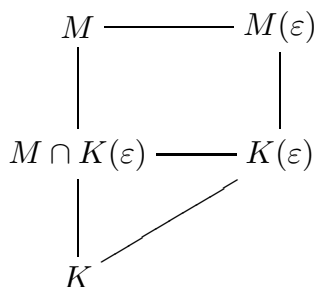
Since  $Gal(M/K)$  is solvable, there exists a normal series  $G \supset G_1 \supset \dots \supset G_{t-1} \supset G_t = \{e\}$  with abelian factors:

$$\begin{array}{ccc}
 M = \mathcal{F}(G_t) & \text{-----} & G_t = \{e\} \\
 | & & | \\
 K_{t-1} = \mathcal{F}(G_{t-1}) & \text{-----} & G_{t-1} \\
 \vdots & & \vdots \\
 K_1 = \mathcal{F}(G_1) & \text{-----} & G_1 \\
 | & & | \\
 K & \text{-----} & G = Gr(M/K)
 \end{array}$$

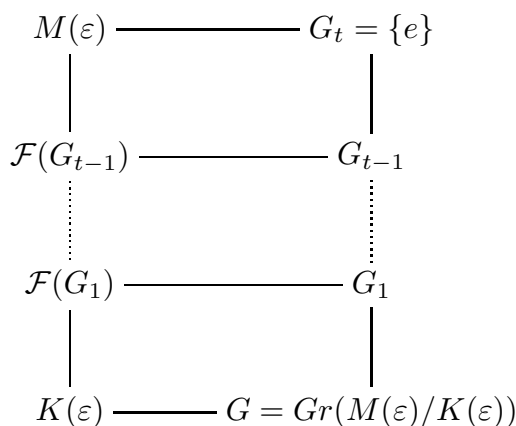
For the corresponding sequence of fixed fields  $K = \mathcal{F}(Gal(M/K)) \subset K_1 = \mathcal{F}(G_1) \subset \dots \subset K_{t-1} = \mathcal{F}(G_{t-1}) \subset M = \mathcal{F}(\{e\})$ , each field is an abelian extension of the previous one, so  $M/K$  is meta-abelian.  $\square$

We now return to the proof of the implication ”i) $\Rightarrow$  iii)” in the main theorem. By the above lemma  $Gal(\widetilde{M}/K)$  is solvable; by the fundamental theorem of Galois theory  $Gal(M/K)$  is a homomorphic image of  $Gal(\widetilde{M}/K)$  and therefore by a Theorem 1.166 also solvable.

”iii) $\Rightarrow$ i)” We now assume that  $\text{Gal}(M/K)$  is solvable. Let  $n = [M : K]$  and let  $\varepsilon$  be a primitive  $n$ -th root of unity. According to the translation theorem applied on



the Galois group  $\text{Gal}(M(\varepsilon)/K(\varepsilon))$  is isomorphic to a subgroup of  $\text{Gal}(M/K)$  and therefore by Theorem 1.166 also solvable.  $\text{Gal}(M(\varepsilon)/K(\varepsilon))$  thus contains a normal series with cyclic factors (consider for instance a composition series; one can then even obtain that the orders of the factors are prime numbers). Let  $G := \text{Gal}(M(\varepsilon)/K(\varepsilon)) \supset G_1 \supset G_2 \supset \dots \supset G_{t-1} \supset (e) = G_t$  be such a series. We then have the following diagram of subfields of  $M(\varepsilon)$  and subgroups of  $G$



Each  $\mathcal{F}(G_i)/\mathcal{F}(G_{i-1})$  is cyclic of an order dividing  $n$ . Since  $\mathcal{F}(G_{i-1})$  contains all  $n$ -th roots of unity Theorem 5.8 implies that there exists  $\alpha_i \in \mathcal{F}(G_i)$  such that  $\mathcal{F}(G_i) = \mathcal{F}(G_{i-1})(\alpha_i)$  where  $\alpha_i^{n_i} \in \mathcal{F}(G_{i-1})$  and  $n_i = [\mathcal{F}(G_i) : \mathcal{F}(G_{i-1})]$ . Therefore  $M(\varepsilon)/K(\varepsilon)$  is a radical extension. Now  $\varepsilon^n = 1$  so  $M(\varepsilon)/K$  is a radical extension in which  $f(x)$  has all its roots. □

DEFINITION 5.18. An irreducible polynomial  $f(x) \in K[x]$  is said to be solvable by radicals (or just solvable) if  $f(x)$  satisfies the equivalent conditions in the above theorem.

-----

**EXPLICIT EXAMPLES.**

In the following we consider polynomials with coefficients in a field  $K$  of characteristic 0 and assume that  $K$  is a subfield of the field  $\mathbb{C}$  of complex numbers.

Let  $f(x)$  be an irreducible polynomial in  $K[x]$  of degree  $n$ . Let  $M$  be the splitting field for  $f(x)$  over  $K$ . By theorem 12 in Chap.III  $\text{Gal}(M/K)$  is isomorphic to a subgroup of  $S_n$ . Therefore  $f(x)$  is solvable by radicals for  $n \leq 4$ . However, the main theorem about solvability by radicals is only an existence theorem: it is not effective in the sense that it does not give a method for explicitly finding the roots of a solvable polynomial expressed by radicals.

The case  $n = 2$  is classical and does not give problems for finding the roots explicitly.

For  $n = 3$  one has Cardano's formula, which we shall now describe.

We first remark quite generally that for solving a polynomial of degree  $n$  we may assume that the coefficient of  $x^{n-1}$  is 0.

Indeed, consider a polynomial of degree  $n$ :

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_{n-1}x + a_n$$

The substitution  $x \rightarrow x - a_1/n$  sends  $f(x)$  into a polynomial, where the coefficient of  $x^{n-1}$  is 0.

For solving a cubic equation  $f(x) = 0$ , we may therefore assume that  $f(x)$  has the form  $x^3 + px + q$ . Cardano's formula expresses the roots as

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

which should be understood as follows: Let  $u$  and  $v$  be chosen, such that  $u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$  and  $v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$  and  $uv = -\frac{p}{3}$ . This is always possible: If  $u$  and  $v$  have the above third powers, then  $u \cdot v$  will be one of the numbers  $-\frac{p}{3}$ ,  $\varepsilon(-\frac{p}{3})$  or  $\varepsilon^2(-\frac{p}{3})$ , where  $\varepsilon$  is a primitive third root of unity. By - if necessary - replacing  $u$  by  $u\varepsilon^2$  or  $u\varepsilon$  one can obtain that the product is  $-\frac{p}{3}$ .

Once  $u$  and  $v$  are chosen as indicated above, the roots of the cubic equation are exactly  $u + v$ ,  $u\varepsilon + v\varepsilon^2$ ,  $u\varepsilon^2 + v\varepsilon$ .

That these numbers really are the roots counted with the right multiplicities follows from the fact that  $f(x)$  can be written

$$f(x) = x^3 + px + q = [x - (u + v)][x - (u\varepsilon + v\varepsilon^2)][x - (u\varepsilon^2 + v\varepsilon)]$$

EXAMPLE 5.19. The cubic equation  $x^3 + 3x + 2 = 0$  has exactly one real root and two complex conjugate roots, since the discriminant  $-4 \cdot 3^3 - 27 \cdot 2^2 = -216$  is negative (cf. Theorem 2.85 in Chap. II). The real root is  $\sqrt[3]{-1 + \sqrt{2}} + \sqrt[3]{-1 - \sqrt{2}}$  and the two complex roots are  $\sqrt[3]{-1 + \sqrt{2}} \cdot \varepsilon + \sqrt[3]{-1 - \sqrt{2}} \cdot \varepsilon^2$  and  $\sqrt[3]{-1 + \sqrt{2}} \cdot \varepsilon^2 + \sqrt[3]{-1 - \sqrt{2}} \cdot \varepsilon$ ,

where  $\varepsilon$  again denotes a primitive third root of unity, for instance  $(-1+i\sqrt{3})/2$ . (The Galois group for the corresponding splitting field over  $\mathbb{Q}$  is the symmetric group  $S_3$ .)

EXAMPLE 5.20. The discriminant of  $x^3 - 3x + 1$  is 81, so the polynomial has three real roots (cf. Theorem 29 in Chap. II). To find these we are looking for numbers  $u$  and  $v$  such that  $u^3 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ ,  $v^3 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$  subject to the condition  $uv = 1$ . If we let  $u_0 = e^{\frac{2\pi i}{9}}$ ,  $v_0 = e^{-\frac{2\pi i}{9}}$  and let  $\varepsilon$  be the primitive third root of unity  $e^{\frac{2\pi i}{3}}$ , then the roots are  $u_0 + v_0 = 2 \cos \frac{2\pi}{9}$ ,  $u_0\varepsilon + v_0\varepsilon^2 = 2 \cos \frac{8\pi}{9}$  and  $u_0\varepsilon^2 + v_0\varepsilon = 2 \cos \frac{14\pi}{9}$ .

The Galois group for the corresponding splitting field over  $\mathbb{Q}$  is the alternating group  $A_3$  ( $\simeq$  the cyclic group of order 3). The splitting field is  $\mathbb{Q}_9 \cap \mathbb{R}$ , i.e. the real numbers lying in the ninth cyclotomic field  $\mathbb{Q}_9$ . (Why?)

REMARK 5.21. If we consider a cubic polynomial  $f(x) = x^3 + px + q$  in  $\mathbb{Q}$  for which the discriminant  $-4p^3 - 27q^2$  is negative,  $f(x)$  has exactly one real root. Since  $\frac{p^3}{27} + \frac{q^2}{4}$  is then positive, Cardanos formula gives an expression of the real root entirely by real radicals.

If however the discriminant  $-4p^3 - 27q^2$  is positive,  $f(x)$  has three real roots. Since  $\frac{p^3}{27} + \frac{q^2}{4}$  is then negative Cardanos formula gives expressions of the three real roots involving non-real complex numbers (and thus essentially trigonometric functions). In this case it can be proved that the roots cannot be expressed entirely by real radicals. This case of cubic equations was called "casus irreducibilis".

For  $n = 4$  we may assume that  $f(x)$  has the form  $x^4 + px^2 + qx + r$ . We may also assume that  $q \neq 0$ , since otherwise  $f(x)$  is just a quadratic polynomial in  $x^2$ . We may write  $f(x)$  as

$$f(x) = (x^2 + u)^2 - [(2u - p)x^2 - qx - (r - u^2)],$$

where we want to choose  $u$  such that the quadratic polynomial in the square bracket becomes a perfect square, i.e. the discriminant vanishes:

$$q^2 - 4(2u - p)(u^2 - r) = 0.$$

This gives rise to a cubic equation in  $u$ . Since  $q \neq 0$  a root  $u$  of this cubic equation must be  $\neq p/2$ . For this root  $u$  we get:

$$f(x) = (x^2 + u)^2 - (2u - p)\left(x - \frac{q}{2(2u - p)}\right)^2$$

and thus

$$f(x) = \left\{ (x^2 + u) + \sqrt{2u - p} \cdot \left(x - \frac{q}{2(2u - p)}\right) \right\} \left\{ (x^2 + u) - \sqrt{2u - p} \cdot \left(x - \frac{q}{2(2u - p)}\right) \right\}$$

The roots of  $f(x)$  can now be found as the roots of two quadratic polynomials.

EXAMPLE 5.22. Let us apply the above procedure at the polynomial  $f(x) = x^4 + 4x - 6$ . We are lead to finding a  $u$  such that  $u^3 + 6u - 2 = 0$ .

By Cardano's formula we find that  $\sqrt[3]{4} - \sqrt[3]{2}$  is an applicable  $u$ . We then get the following factorization of  $f(x)$ :

$$f(x) = \left[x^2 - \sqrt{2u}x + u + \frac{\sqrt{2u}}{u}\right] \left[x^2 + \sqrt{2u}x + u - \frac{\sqrt{2u}}{u}\right]$$

which immediately leads to the following explicit expressions for the roots of  $f(x)$ :

$$\sqrt{\frac{u}{2}} \pm \sqrt{-\frac{u}{2} - \sqrt{\frac{2}{u}}} \quad \text{og} \quad -\sqrt{\frac{u}{2}} \pm \sqrt{-\frac{u}{2} + \sqrt{\frac{2}{u}}}$$

where  $u = \sqrt[3]{4} - \sqrt[3]{2}$ .

(Make a guess: what is the Galois group for the splitting field for  $f(x)$  over  $\mathbb{Q}$ ?)

### POLYNOMIALS OF DEGREE $\geq 5$ .

For the proof of the main result of this section we shall need a group theoretical lemma.

**Lemma 5.23.** *Let  $p$  be a prime number and  $\mathfrak{p}$  a transitive subgroup of the symmetric group  $S_p$ . If  $\mathfrak{p}$  contains a transposition then  $\mathfrak{p} = S_p$ .*

*Proof.* The proof goes in five steps:

i) In the set  $\{1, 2, \dots, p\}$  we introduce an equivalence relation by  $a \sim b$  iff  $a = b$  or the transposition  $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$  lies in  $\mathfrak{p}$ .

[Verify that this really is an equivalence relation.]

ii) If  $a \sim b$  and  $\tau \in \mathfrak{p}$  then  $\tau(a) \sim \tau(b)$ .

[Indeed: if  $a \sim b$  and  $a \neq b$  then the transposition  $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$  lies in  $\mathfrak{p}$ . Since  $\mathfrak{p}$  is a subgroup and  $\begin{pmatrix} \tau a & \tau b \\ \tau b & \tau a \end{pmatrix} = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \tau^{-1}$  it follows that  $\tau(a) \sim \tau(b)$ .]

iii) All the equivalence classes have the same number of elements.

[Indeed: let  $S = \{a_1, \dots, a_s\}$  and  $T = \{b_1, \dots, b_t\}$  be two arbitrary equivalence classes. Since  $\mathfrak{p}$  is transitive, there is a  $\sigma \in \mathfrak{p}$  such that  $\sigma(a_1) = b_1$ . Therefore - by ii) - all the elements  $b_1 = \sigma(a_1), \sigma(a_2), \dots, \sigma(a_s)$  will lie in the equivalence class  $T$ . In particular,  $s \leq t$ . Quite similarly we get  $t \leq s$ . Consequently  $s = t$ .]

iv) There is just one equivalence class.

[Indeed:  $p = (\text{number of equivalence classes}) \cdot (\text{the common number of elements in the equivalence classes})$ . Since  $\mathfrak{p}$  contains a transposition, the last factor is  $\geq 2$ . Because  $p$  is a prime number this factor must be  $p$ . Therefore there is just one equivalence class.]

v)  $\mathfrak{p} = S_p$ .

[Indeed: since any two elements in the set  $\{1, 2, \dots, p\}$  are equivalent,  $\mathfrak{p}$  contains all transpositions. Since every permutation in  $S_p$  is a product of transpositions we conclude that  $\mathfrak{p} = S_p$ .]  $\square$

**Theorem 5.24.** *Let  $f(x)$  be an irreducible polynomial in  $\mathbb{Q}[x]$  of degree  $p$ , where  $p$  is a prime number and let  $M$  be the splitting field of  $f(x)$  over  $\mathbb{Q}$ . If  $f(x)$  has exactly  $(p - 2)$  real roots, then  $\text{Gal}(M/\mathbb{Q})$  is isomorphic to the symmetric group  $S_p$ , and therefore  $f(x)$  is not solvable by radicals when  $p \geq 5$ .*

*Proof.* By Theorem 3.40 in Chap. III the Galois group  $\text{Gal}(M/\mathbb{Q})$  is isomorphic to a transitive subgroup of  $S_p$ . The complex conjugation  $\tau$  is an automorphism in  $\text{Gal}(M/\mathbb{Q})$  that corresponds to a transposition in  $S_p$ .

(It fixes the  $p - 2$  real roots and permutes the two complex conjugate roots.) The previous lemma implies that  $\text{Gal}(M/\mathbb{Q}) \simeq S_p$ .  $\square$

EXAMPLE 5.25.  $f(x) = x^5 - 4x + 2$  is irreducible over  $\mathbb{Q}$  (by Eisenstein's criterion). Since  $f(-\infty) < 0$ ,  $f(0) > 0$ ,  $f(1) < 0$ ,  $f(+\infty) > 0$ , we conclude that  $f(x)$  has at least 3 real roots. Because  $f(x)$  has degree 5, the number of real roots must be 3 or 5. If  $f(x)$  had 5 real roots, then by Rolle's theorem  $f'(x) = 5x^4 - 4$  would have 4 real roots. Since  $f'(x)$  has only 2 real roots,  $f(x)$  has exactly 3 real roots.

Therefore  $f(x)$  is not solvable by radicals!

We show more generally

**Theorem 5.26.** *For every odd prime number  $p$  there exists a normal extension of  $\mathbb{Q}$  with  $S_p$  as Galois group.*

*Proof.* By virtue of Theorem 5.24 it is enough to show that there exists an irreducible polynomial in  $\mathbb{Q}[X]$  of degree  $p$  having exactly  $p - 2$  real roots.

For all sufficiently large natural numbers  $t$  the polynomial

$$f(x) = (x^2 + 1)(x - 1)(x - 2) \dots (x - (p - 2)) + 2/2^{tp}$$

has exactly  $p - 2$  real roots. We have to show that  $f(x)$  is irreducible in  $\mathbb{Q}[X]$ . For this it suffices to verify that

$$2^{tp} f(x/2^t) = (x^2 + 2^{2t})(x - 2^t)(x - 2 \cdot 2^t) \dots (x - (p - 2) \cdot 2^t) + 2$$

is irreducible. But here Eisenstein's criterion can be used with the prime number 2.  $\square$

**Theorem 5.27.** *For every finite group  $G$  there exists a normal extension  $M/L$ , where  $\text{Gal}(M/L) \simeq G$  and  $L$  is a finite extension of  $\mathbb{Q}$ .*

*Proof.* If  $G$  has order  $n$  then by Cayley's theorem  $G$  is isomorphic to a subgroup of the symmetric group  $S_n$ . Since there exist infinitely many prime numbers there exists a prime  $p \geq n$ . Then  $G$  is also isomorphic to a subgroup of the symmetric group  $S_p$ .

By Theorem 5.26 there exists a normal extension  $M$  of  $\mathbb{Q}$  for which  $\text{Gal}(M/\mathbb{Q}) \simeq S_p$ .

The fixed field  $L = \mathcal{F}(G)$  is a finite extension of  $\mathbb{Q}$  and  $M/L$  is a finite normal extension having  $G$  as Galois group.  $\square$

### CONCLUDING REMARKS.

The above theorem shows that it is fairly easy to realize an arbitrary finite group  $G$  as Galois group over some finite extension  $L$  of  $\mathbb{Q}$ . The inverse problem of Galois theory, i.e. the question whether every finite group can be realized as a Galois group over  $\mathbb{Q}$ , may therefore be viewed as a sort of "descent problem". We "just" have to replace  $L$  by  $\mathbb{Q}$ .

This is an extremely difficult problem, where one still has only sporadic results. It is for instance not even known if there exists a fixed finite extension  $L$  of  $\mathbb{Q}$ , such that every finite group can be realized as a Galois group over  $L$ .

However it can be shown that there exists an infinite algebraic extension of  $\mathbb{Q}$ , over which every finite group can be realized as a Galois group.

*And the end of all our exploring  
Will be to arrive where we started  
And know the place for the first time.*

(T.S. Eliot, Little Gidding)

