Fields and the Galois theory

April 21, 2024

Table of Contents

1. Algebraic extensions of fields

1.1. Fields, prime subfield, characteristic

1.1.1. *A field* is a commutative division ring, that is, a commutative unital ring in which all nonzero elements are units.

1.1.2. Examples of fields.

(i) $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

(ii) $\mathbb{F}_p = \mathbb{Z}_p = \mathbb{Z}/(p)$, where p is a prime integer.

(iii) For any integral domain we have its field of fractions.

(iv) Here are special cases of (iii): for any field F we have the field $F(x)$ of rational functions in one variable, and for every n, the field $F(x_1, \dots, x_n)$ of rational functions in n variables.

(v) Let R be a commutative ring and M be a maximal ideal in R; then R/M is a field.

(vi) A special case of (v): Let F be a field and let $f \in F[x]$ be an irreducible polynomial. Then $F[x]/(f)$ is a field.

1.1.3. Fields have no nontrivial ideals. Hence, factorization is not defined on fields, "quotient fields" do not exist. Any (nonzero) homomorphism of fields is a monomorphism.

1.1.4. Let F be a field, and let P be the cyclic additive subgroup of F generated by 1. There are two cases:

Case 1. P is finite. Then $P \cong \mathbb{Z}_p$ for some prime $p \in \mathbb{N}$, and P is a field isomorphic to $\mathbb{F}_p$; it is called *the prime subfield* of F. In this case we say that F *has characteristic* p, write $\operatorname{char} F = p$, and say that F has *finite characteristic*.

Case 2. P is infinite, $\cong \mathbb{Z}$. Then P is contained in (and generates) a subfield of F isomorphic to $\mathbb{Q}$, which is, again, called the prime subfield of F. We say that F *has characteristic* 0 in this case and write $\operatorname{char} F = 0$.

In both cases, of a finite and of zero characteristic, the prime subfield is the minimal subfield of F, contained in all other subfields of F.

1.2. Extensions and subextensions

1.2.1. If K is a field and F is a subfield of K, we say that K is *an extension* of F, and write K/F or $\begin{matrix} K \\ | \\ F \end{matrix}$. (More exactly, *an extension* is a pair (K, F) of fields with $F \subseteq K$.)

1.2.2. If F is a subfield of L and L is a subfield of K, then we say that L/F is *a subextension* of the extension K/F.

1.2.3. The intersection of any family of subfields of a field K is a subfield of K; if all these fields are extensions of a subfield F of K, then their intersection is an extension of F.

1.2.4. If K/F is an extension and S is a subset of K, $F[S]$ denotes the F-algebra generated by S,

$$F[S] = \Big\{ f(\alpha_1, \dots, \alpha_n) : n \geq 0,\ f \in F[x_1, \dots, x_n],\ \alpha_1, \dots, \alpha_n \in S \Big\}.$$

If S is finite, $S = \{\alpha_1, \dots, \alpha_n\}$, we write $F[\alpha_1, \dots, \alpha_n]$ for $F[S]$.

1.2.5. Let K/F be an extension and let S be a subset of K. Then $F(S)$ is the minimal extension of F that contains S; it is called *the extension of F generated by S*. ($F(S)$ is the intersection of all extensions of F that contain S.) $F(S)$ contains the ring $F[S]$ and is (isomorphic to) the field of fractions of $F[S]$: $F(S) = \{\alpha/\beta : \alpha, \beta \in F[S],\ \beta \neq 0\}$.

If $K = F(S)$ for a finite set S, we say that the extension K/F is *finitely generated*. If S is a finite set, $S = \{\alpha_1, \dots, \alpha_n\}$, then we write $F(\alpha_1, \dots, \alpha_n)$ for $F(S)$.

1.2.6. A sequence $K_n/K_{n-1}/\cdots/K_1/F$ of successive extensions is called *a tower* of extensions. Abusing language, we also say in this situation that K_n is a tower of extensions.

1.2.7. If L_1 and L_2 are subfields of a field K, then the field $L_1(L_2) = L_2(L_1)$ (the minimal extension of both L_1 and L_2) is called *the composite* of L_1 and L_2 and is denoted by L_1L_2.

1.2.8. We have the following *diamond diagram* of extensions:

$$\begin{array}{ccc} & L_1L_2 & \\ \swarrow & & \searrow \\ L_1 & & L_2 \\ \searrow & & \swarrow \\ & L_1 \cap L_2. & \end{array}$$

Notice that this is the minimal such diagram, in the sense that if

$$\begin{array}{ccc} & K & \\ \swarrow & & \searrow \\ L_1 & & L_2 \\ \searrow & & \swarrow \\ & L & \end{array}$$

is another diagram of extensions with the same L_1 and L_2, then K is an extension of L_1L_2 and L is a subfield of $L_1 \cap L_2$:

$$\begin{array}{ccc} & K & \\ & | & \\ & L_1L_2 & \\ \swarrow & & \searrow \\ L_1 & & L_2 \\ \searrow & & \swarrow \\ & L_1 \cap L_2 & \\ & | & \\ & L. & \end{array}$$

1.3. Finite extensions

1.3.1. If K/F is an extension, then K is an F-vector space (and an F-algebra). The dimension $\dim_F K$ of K is called *the degree* of this extension, or the degree of K over F, and is denoted by $[K : F]$.

If $[K : F] < \infty$, K/F is said to be *a finite extension*, and is said to be *an infinite extension* otherwise.

In diagrams of extensions, the degree $n = [K : F]$ appears this way: $\begin{array}{c} K \\ {\scriptstyle n}| \\ F. \end{array}$

1.3.2. An extension of degree 2 is said to be *quadratic*, of degree 3 *cubic*, of degree 4 *quartic*, of degree 5 *quintic*, etc.

1.3.3. Theorem. *Let $K/L/F$ be a tower of extensions. If B is a basis of L over F and C is a basis of K over L, then $CB = \{\gamma\beta : \gamma \in C,\ \beta \in B\}$ is a basis of K over F.*

Proof. Every $\alpha \in K$ is representable as a finite sum $\alpha = \sum_{\gamma \in C} \alpha_\gamma \gamma$ with $\alpha_\gamma \in L$ for all γ. (It is assumed that all but finitely many α_γ are equal to 0.) For each $\gamma \in C$, α_γ is representable as a finite sum $\alpha_\gamma = \sum_{\beta \in B} a_{\gamma,\beta}\beta$ with $a_{\gamma,\beta} \in F$ for all β. So, $\alpha = \sum_{\substack{\gamma \in C \\ \beta \in B}} a_{\beta,\gamma}\gamma\beta$. So, the set CB spans K as an F-vector space.

Let's now assume that a (finite) linear combination $\sum_{\substack{\gamma \in C \\ \beta \in B}} a_{\beta,\gamma}\gamma\beta = 0$ where $a_{\gamma,\beta} \in F$ for all γ and β. then $\sum_{\gamma \in C} \alpha_\gamma \gamma = \sum_{\gamma \in C} \sum_{\beta \in B} a_{\beta,\gamma}\gamma\beta = 0$, where for each γ, $\alpha_\gamma = \sum_{\beta \in B} a_{\beta,\gamma}\beta \in L$. This implies that $\alpha_\gamma = 0$ for every γ. But then, for every γ, $a_{\beta,\gamma} = 0$ for every β. Hence, the set CB is linearly independent over F. ■

1.3.4. Corollary. *If K/L and L/F are finite extensions, then K/F is also finite, with $[K : F] = [K : L] \cdot [L : F]$.*

1.3.5. Corollary. *If L/F is a subextension of a finite extension K/F, then both K/L and L/F are finite, with $[K:L]\,\big|\,[K:F]$ and $[L:F]\,\big|\,[K:F]$.*

1.4. Simple extensions

1.4.1. An extension K/F is said to be *simple* if it is generated by a single element: $K = F(\alpha)$ for some $\alpha \in K$.

1.4.2. Let K/F be an extension and let $\alpha \in K$. We then have an F-algebras homomorphism $\varphi\colon F[x] \longrightarrow K$ sending x to α and every $f \in F[x]$ to $f(\alpha)$. The subring $\varphi(F[x]) = \{f(\alpha), f \in F[x]\}$ of K is denoted by $F[\alpha]$, and we have $F[\alpha] \cong F[x]/\ker\varphi$.

1.4.3. Let K/F be a simple extension, $K = F(\alpha)$, and let $\varphi\colon F[x] \longrightarrow K$ be the homomorphism that maps x to α. There can be two cases:

Case 1: $\ker\varphi \neq 0$.
Then $\ker\varphi$ is a maximal ideal in $F[x]$, generated by an irreducible polynomial p, $F[\alpha]$ is a field, so $K = F[\alpha]$. Thus, $K = \big\{f(\alpha),\ f \in K[x],\ \deg f \leq n-1\big\}$ where $n = \deg p$, with the basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ over F, and $[K:F] = n$.

In this case:

(i) We say that the element α is *algebraic* over F.

(ii) We call the irreducible polynomial p *the minimal polynomial* of α and denote it by $m_{\alpha,F}$ or just m_α. The minimal polynomial $m_{\alpha,F}$ of α is defined uniquely up to multiplication by scalars; it is usually assumed that it is monic. We have $m_\alpha(\alpha) = 0$, and $f(\alpha) = 0$ for $f \in K[x]$ iff $m_\alpha \,\big|\, f$. m_α is the only irreducible polynomial such that $m_\alpha(\alpha) = 0$.

(iii) We call the degree of m_α (which is also the degree $[K:F]$) *the degree of α over F* and denote it by $\deg_F \alpha$.

Case 2: $\ker\varphi = 0$. In this case K contains the copy $F[\alpha] = \varphi(F[x])$ of the ring $F[x]$, and is its field of fractions, so that $F(\alpha) \cong F(x)$, the field of rational functions over F. We then have $[K:F] = \infty$.

In this case, we say that α is *transcendental* over F.

1.4.4. If K/F is a finite extension then for every $\alpha \in K$, $\deg_F \alpha \,\big|\, [K:F]$.

1.4.5. Let K/F be a finite extension and let $\alpha \in K$. Here are some methods of finding the minimal polynomial $m_{\alpha,F}$ of an element α algebraic over F:

(i) Find a "small" nonzero polynomial f satisfying $f(\alpha) = 0$ and prove that it is irreducible.

(ii) Write the powers of α in coordinates with respect to a basis of K over F, and find the minimal linear dependence relation between them.

(iii) The action of α on K by multiplication, $u \mapsto \alpha u$, is a linear transformation of the finite dimensional F-vector space K; let's denote it by T. Let $K = W_1 \oplus \cdots \oplus W_d$ be the decomposition of K into a direct sum of cyclic T-invariant subspaces, and let $p_1, \ldots, p_d$ be the invariant factors of T. The actions of T on W_i are all isomorphic, so all invariant factors are equal, $p_1 = \ldots = p_d$, and the minimal polynomial of T (and so, of α) is p_1.

(iv) It follows from (iii) that the characteristic polynomial c_T of T is m_α^d. so, m_T is the irreducible polynomial for which $c_T = m_\alpha^d$.

(iv) See also subsection 6.1.1 below.

1.5. Towers of simple extensions

1.5.1. Any finitely generated extension K/F is a tower of simple extensions: if $K = F(\alpha_1, \ldots, \alpha_n)$ then we have the tower $K = K_n/K_{n-1}/\cdots/K_1/K_0 = F$, where for each i, $K_i = F(\alpha_1, \ldots, \alpha_i)$, and so, $K_i = K_{i-1}(\alpha_i)$.

1.5.2. If L/F is a subextension of an extension K/F and $\alpha \in K$ is algebraic over F, then α is algebraic over L as well, and $m_{\alpha,L} \,\big|\, m_{\alpha,F}$, so $\deg_L \alpha = \deg m_{\alpha,L} \leq \deg m_{\alpha,F} = \deg_F \alpha$.

1.5.3. It follows from Theorem 1.3.3 by induction on n that

Theorem. *If $K = F(\alpha_1, \dots, \alpha_n)$ and $\alpha_1, \dots, \alpha_n$ are algebraic over F, then $K = F[\alpha_1, \dots, \alpha_n]$ and*

$$[K : F] = \prod_{i=1}^{n} \deg_{F(\alpha_1,\dots,\alpha_{i-1})} \alpha_i \le \prod_{i=1}^{n} \deg_F \alpha_i.$$

Proof. We have

$$K = F(\alpha_1)(\alpha_2)\dots(\alpha_n) = F[\alpha_1][\alpha_2]\dots[\alpha_n] = F[\alpha_1, \dots, \alpha_n].$$

The second part immediately follows from Corollary 1.3.4 and 1.5.2. ■

1.6. The composite of two finite extensions

1.6.1. If K/F is a finite extension, then it is generated by finitely many algebraic elements, and is a tower of finite simple extensions.

1.6.2. Theorem. *If L_1/F and L_2/F are two finite subextensions of an extension K/F, then their composite L_1L_2 is also a finite extension of F, with $[L_1L_2 : F] \le [L_1 : F] \cdot [L_2 : F]$. If, as F-vector spaces, L_1 is spanned by a set $\{\alpha_1, \dots, \alpha_n\}$ and L_2 by a set $\{\beta_1, \dots, \beta_m\}$, then L_1L_2 is spanned over F by the set $\{\alpha_i\beta_j,\ i = 1, \dots, n,\ j = 1, \dots, m\}$.*

Proof. We have $L_1L_2 = F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m) = F[\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m]$, which is the F-algebra generated by L_1 and L_2. The elements of this algebra are linear combinations, with coefficients from F, of products $\alpha\beta$ with $\alpha \in L_1$ and $\beta \in L_2$, and for such a product, if $\alpha = \sum_{i=1}^{n} a_i\alpha_i$ and $\beta = \sum_{j=1}^{m} b_j\beta_j$ with $a_i, b_j \in F$, we have $\alpha\beta = \sum_{i,j} a_ib_j\alpha_i\beta_j$. Hence, every element of L_1L_2 is a linear combination of the elements $\alpha_i\beta_j$ with coefficients from F. ■

1.6.3. Let L_1/F and L_2/F be two finite subextensions of an extension K/F, with $[L_1 : F] = n$ and $[L_2 : F] = m$. Then in the diamond diagram

$$\begin{array}{ccc} & L_1L_2 & \\ {\scriptstyle m'}\swarrow & & \searrow{\scriptstyle n'} \\ L_1 & & L_2 \\ {\scriptstyle n}\searrow & & \swarrow{\scriptstyle m} \\ & L_1 \cap L_2. & \end{array}$$

we have $nm' = n'm$, $n' \le n$, and $m' \le m$. If n and m are coprime, then $n' = n$ and $m' = m$.

1.6.4. It follows that for two finite subextensions L_1/F and L_2/F of an extension K/F the F-algebras homomorphism $L_1 \otimes_F L_2 \longrightarrow L_1L_2$ is surjective. In the case $[L_1L_2 : F] = [L_1 : F] \cdot [L_2 : F]$, this is an isomorphism, and if $\{\alpha_1, \dots, \alpha_n\}$ is a basis of L_1 over F and $\{\beta_1, \dots, \beta_m\}$ is a basis of L_2, then $\{\alpha_i\beta_j,\ i = 1, \dots, n,\ j = 1, \dots, m\}$ is a basis of L_1L_2.

1.7. Quadratic and biquadratic extensions

1.7.1. An extension K/F with $[K : F] = 2$ is said to be *quadratic*.

1.7.2. Let F be a field with $\operatorname{char} F \ne 2$, and let K/F be a quadratic extension. Then $K = F(\sqrt{d})$ for some $d \in F$. (Under $\sqrt{d}$ we understand any element δ of any extension of F such that $\delta^2 = d$.) Indeed, let α be any element of $K \setminus F$; then $\deg_F \alpha = 2$, so α is a root of a quadratic polynomial $p = x^2 + ax + b$ with $a, b \in F$, $\alpha^2 + a\alpha + b = 0$. Then $(\alpha + a/2)^2 = d$, where $d = a^2/4 - b$. (d is *the discriminant* of p(!).) So, $\sqrt{d} = \alpha + a/2 \in K$, and $K = F(\sqrt{d})$. The set $\{1, \sqrt{d}\}$ is a basis of K over F.

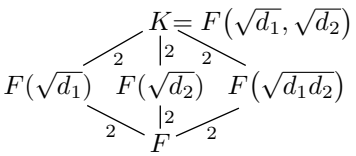
1.7.3. Let F be a field with $\operatorname{char} F \ne 2$, and let K/F be quadratic, $K = F(\sqrt{d})$. An element $\alpha \in K$ satisfies $\alpha^2 \in F$ iff $\alpha \in F$ or $\alpha \in F\sqrt{d}$ (that is, $\alpha = b\sqrt{d}$ for some $b \in F$). Indeed, every $\alpha \in K$ has form $a + b\sqrt{d}$ with $a, b \in F$, then $\alpha^2 = a^2 + b^2d + 2ab\sqrt{d}$, and we have $\alpha^2 \in F$ iff $ab = 0$, so either $d = a$, or $d = b\sqrt{d}$.

1.7.4. An extension K/F with $[K : F] = 4$ is said to be *quartic*.

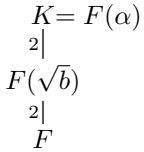
1.7.5. A quartic extension K/F is called *biquadratic* if it is representable as a composite of two quadratic extensions, $K = L_1L_2$ with $[L_1 : F] = [L_2 : F] = 2$. Assume that $\operatorname{char} F \neq 2$, then $L_1 = F(\sqrt{d_1})$ and $L_2 = F(\sqrt{d_2})$ for some $d_1, d_2 \in F$, and $K = F\big(\sqrt{d_1}, \sqrt{d_2}\big)$ for some $d_1, d_2 \in F$, with $\sqrt{d_1}, \sqrt{d_2} \notin F$; for K/F to be quartic it is also necessary and sufficient that $L_1 \neq L_2$, that is, $\sqrt{d_2} \neq c\sqrt{d_1}$ with $c \in F$, which is equivalent to $\sqrt{d_1d_2} \notin F$.

The set $\big\{1, \sqrt{d_1}, \sqrt{d_2}, \sqrt{d_1d_2}\big\}$ is a basis of K over F.

1.7.6. Let $\operatorname{char} F \neq 2$ and K/F be biquadratic, $K = F\big(\sqrt{d_1}, \sqrt{d_2}\big)$. By 1.7.3, for $\alpha \in K$ we have $\alpha^2 \in F(\sqrt{d_1})$ iff $\alpha \in F(\sqrt{d_1})$ or $\alpha \in F(\sqrt{d_1})\sqrt{d_2}$, and $\alpha^2 \in F(\sqrt{d_2})$ iff $\alpha \in F(\sqrt{d_2})$ or $\alpha \in F(\sqrt{d_2})\sqrt{d_1}$. It follows that $\alpha^2 \in F$ iff $\alpha \in F$, or $\alpha \in F\sqrt{d_1}$, or $\alpha \in F\sqrt{d_2}$, or $\alpha \in F\sqrt{d_1d_2}$. (These are one-dimensional intersections of the two-dimensional subspace $F(\sqrt{d_1})$ or $F(\sqrt{d_1})\sqrt{d_2}$ with the two-dimensional subspace $F(\sqrt{d_2})$ or $F(\sqrt{d_2})\sqrt{d_1}$.) Since every nontrivial proper subextension of a biquadratic extension must be quadratic, here is the complete diagram of all subextensions of K/F:



1.7.7. Let now $\operatorname{char} F \neq 2$ and K/F be a tower of two quadratic extensions, $K = F(\alpha)$ where $\alpha = \sqrt{a + \sqrt{b}}$ for some $a, b \in F$ such that $\sqrt{b} \notin F$ and $\alpha \notin F(\sqrt{b})$.



Claim. *K/F is biquadratic iff $a^2 - b = c^2$ for some $c \in F$.*

Proof. Let K/F be biquadratic, $K = F\big(\sqrt{d_1}, \sqrt{d_2}\big)$. Since $(\sqrt{b})^2 \in F$ and $\sqrt{b} \notin F$, we have $\sqrt{b} \in F\sqrt{d_1}$, $F\sqrt{d_2}$ or $F\sqrt{d_1d_2}$. W.l.o.g. assume that $\sqrt{b} \in F\sqrt{d_1}$. Then $\alpha^2 = a + \sqrt{b} \in F(\sqrt{d_1})$ and $\alpha \notin F(\sqrt{d_1})$, so $\alpha \in F(\sqrt{d_1})\sqrt{d_2}$, $\alpha = x\sqrt{d_2} + y\sqrt{d_1d_2}$ for sme $x, y \in F$. Then $a + \sqrt{b} = \alpha^2 = x^2d_2 + y^2d_1d_2 + 2xyd_2\sqrt{d_1}$, so $a = x^2d_2 + y^2d_1d_2$ and $\sqrt{b} = 2xyd_2\sqrt{d_1}$, thus

$$a^2 - b = \big(x^2d_2 + y^2d_1d_2\big)^2 - 4x^2y^2d_2^2d_1 = \big(x^2d_2 - y^2d_1d_2\big)^2.$$

Conversely, assume that $a^2 - b = c^2$ for $c \in F$. Put $d_1 = \frac{1}{2}(a + c)$ and $d_2 = \frac{1}{2}(a - c)$; then $a = d_1 + d_2$, $c = d_1 - d_2$, $b = a^2 - c^2 = 4d_1d_2$, and we have

$$\alpha^2 = a + \sqrt{b} = d_1 + d_2 + 2\sqrt{d_1d_2} = \big(\sqrt{d_1} + \sqrt{d_2}\big)^2,$$

and $\alpha = \pm\big(\sqrt{d_1} + \sqrt{d_2}\big)$. Hence, $\alpha \in F\big(\sqrt{d_1}, \sqrt{d_2}\big)$, and so $K \subseteq F\big(\sqrt{d_1}, \sqrt{d_2}\big)$; since $[K : F] = 4$ and $\big[F\big(\sqrt{d_1}, \sqrt{d_2}\big) : F\big] \leq 4$, we obtain that $K = F\big(\sqrt{d_1}, \sqrt{d_2}\big)$. ∎

1.8. Algebraic extensions

1.8.1. An extension K/F is said to be *algebraic* if every $\alpha \in K$ is algebraic over F, and is called *transcendental* otherwise.

1.8.2. Theorem. *Any finite extension is algebraic. An algebraic extension is finite iff it is finitely generated. Moreover, an extension is finite if it is generated by finitely many algebraic elements.*

Proof. If K/F is a finite extension, then every element of K has a finite degree over F, and so, is algebraic over F. Also, K has a finite basis, is generated by the elements of this basis, so is finitely generated.

Conversely, if K/F is a finitely generated algebraic extension, or is only generated by finitely many algebraic elements: $K = F(\alpha_1, \dots, \alpha_k)$ where $\alpha_1, \dots, \alpha_k$ are algebraic over F, then K is the composite $K = F(\alpha_1) \cdots F(\alpha_k)$ of finite extensions, and so, is finite. ■

1.8.3. We know that towers and composites of finite extensions are finite. Since algebraic extensions are unions of finite extensions, it follows that towers and composites of algebraic extensions are algebraic:

Theorem. *If K/L and L/F are algebraic extensions, then K/F is algebraic. If L_1/F and L_2/F are two algebraic subextensions of an extension of F, then $(L_1L_2)/F$ is algebraic. Moreover, if an extension K/F is generated by algebraic elements, then it is algebraic.*

Proof. Let K/L and L/F be algebraic extensions, and let $\alpha \in K$; then α is algebraic over L and we need to show that α is algebraic over F. Let $m_{\alpha,L} = x^n + \beta_{n-1}x^{n-1} + \cdots + \beta_1 x + \beta_0 \in L[x]$ be the minimal polynomial of α over L; then it is also the minimal polynomial of α over the field $L' = F(\beta_0, \dots, \beta_{n-1})$. L'/F is a finitely generated algebraic extension, so it is finite; α is algebraic over L', so the extension $L'(\alpha)/L'$ is also finite; thus, $L'(\alpha)/F$ is finite, and α is algebraic over F.

Assume that K/F is generated by a set S of elements algebraic over F, and let $\alpha \in K$. Then α is a rational function, with coefficients from F, of finitely many elements $\beta_1, \dots, \beta_k$ of S. Thus, $\alpha \in F(\beta_1, \dots, \beta_k)$, which is a finite extension of F; so, α is algebraic over F.

Now let L_1/F and L_2/F be two algebraic subextensions of an extension K/F. Then the composite extension $(L_1L_2)/F$ is generated by elements of L_1 and L_2, which are algebraic over F, so $(L_1L_2)F$ is algebraic. ■

1.8.4. Let K/F be an extension. Then the set $E = \{\alpha \in K : \alpha \text{ is algebraic over } F\}$ is a subfield of K: indeed, for any $\alpha_1, \alpha_2 \in E$, $\alpha_1 \pm \alpha_2$, $\alpha_1\alpha_2$, α_1/α_2 are contained in the algebraic extension $F(\alpha_1, \alpha_2)$, and so, are algebraic over F and are contained in E. Since E contains all elements of K algebraic over F, E/F is the maximal algebraic subextension of K/F. Any element $\alpha \in K \setminus E$ is transcendental over E, since otherwise it is algebraic over F. Thus, any extension K/F decomposes into a tower $K/E/F$ where E/F is algebraic and K/E is transcendental with no algebraic elements.

1.8.5. Real numbers, algebraic over $\mathbb{Q}$, are called *algebraic numbers*. Algebraic numbers form a subfield A of $\mathbb{R}$. The field A is countable (it consists of roots of polynomials with rational coefficients, the set of such polynomials is countable, and each polynomial has only finitely many roots), so "almost all" real numbers are *transcendental*.

---

2. Adjoining roots and splitting fields

2.1. Adjoining roots of polynomials and conjugate elements

2.1.1. If K/F is an extension, $f \in F[x]$ is a polynomial, and $\alpha \in K$ is such that $f(\alpha) = 0$, we say that α *is a root of* f. An element $\alpha \in K$ is a root of some nonzero $f \in F[x]$ iff α is algebraic over F and the minimal polynomial $m_{\alpha,F}$ of α over F divides f. In any extension of F, a nonzero polynomial $f \in F[x]$ cannot have more than $\deg f$ roots.

2.1.2. If $\varphi\colon A_1 \longrightarrow A_2$ is a mapping and $B \subseteq A_1 \cap A_2$, we say that φ *fixes* B if $\varphi(a) = a$ for every $a \in B$.

If K_1/F and K_2/F are two extensions of a field F, *a homomorphism* $K_1/F \longrightarrow K_2/F$, or a homomorphism $K_1 \longrightarrow K_2$ *over* F, is a homomorphism $\varphi\colon K_1 \longrightarrow K_2$ that fixes F:

$$\begin{array}{ccc} K_1 & \xrightarrow{\varphi} & K_2. \\ & \searrow \quad \swarrow & \\ & F & \end{array}$$

A homomorphism of extensions is either an isomorphism, or a proper embedding.

2.1.3. Theorem. *Let K_1/F and K_2/F be two extensions of a field F, let $f \in F[x]$ be irreducible, and let $\alpha_1 \in K_1$ and $\alpha_2 \in K_2$ be roots of f. Then both $F(\alpha_1)$ and $F(\alpha_2)$ are isomorphic to $F[x]/(p)$ under isomorphisms that fix F and map α_1 and α_2 to x, so $F(\alpha_1)/F \cong F(\alpha_2)/F$ under an isomorphism that maps α_1 to α_2:*

$$\begin{array}{ccc} F(\alpha_1) & \xrightarrow{\sim} & F(\alpha_2), \quad \alpha_1 \leftrightarrow \alpha_2. \\ & \diagdown \quad \diagup & \\ & F & \end{array}$$

Conversely, if $\varphi\colon K_1/F \longrightarrow K_2/F$ is a homomorphism of extensions of a field F and $\alpha_1 \in K_1$ is algebraic over F, then $\alpha_2 = \varphi(\alpha_1) \in K_2$ is also algebraic over F and has the same minimal polynomial, $m_{\alpha_2,F} = m_{\alpha_1,F}$.

Proof. This is very easy: Both $F(\alpha_1)$ and $F(\alpha_2)$ are isomorphic to $F[x]/(p)$, where isomorphisms $\varphi_i\colon F[x]/(p) \longrightarrow F(\alpha_i)$ are defined by $f \bmod p \longrightarrow f(\alpha_i)$, $i = 1, 2$. In particular, φ_i fix F and map $x \bmod p$ to α_i.

$$\begin{array}{ccccc} F(\alpha_1) & \xleftarrow{\varphi_1} & F[x]/(p) & \xrightarrow{\varphi_2} & F(\alpha_2), \quad \alpha_1 \leftrightarrow x \bmod p \leftrightarrow \alpha_2. \\ & \diagdown & \vert & \diagup & \\ & & F & & \end{array}$$

So, $\varphi_2 \circ \varphi_1^{-1}$ is an isomorphism $F(\alpha_1) \longrightarrow F(\alpha_2)$ that fixes F and maps α_1 to α_2. ∎

2.1.4. If $K = F(\alpha)$ where α is a root of an irreducible polynomial $f \in F[x]$, we say that K *is obtained from F by adjoining a root of f*. Such a field K is unique up to isomorphism.

2.1.5. Now let F be a field and $f \in F[x]$ be an irreducible polynomial. Is there always a field, an extension of F, where f has a root? (We know that this is so for polynomials over $\mathbb{Q}$ or $\mathbb{R}$, any such polynomial has a root in $\mathbb{C}$.) Well, if we don't have such an extension, we can always construct it artificially. Put $K = F[x]/(f)$; since p is irreducible and $F[x]$ is a PID, the ideal (f) is prime and maximal, and K is a field. Let $\alpha \in K$ be the class of x modulo f in K, then $p(\alpha) = f(x) \bmod f = 0$, so α is a root of f in K. Since f is irreducible, f is the minimal polynomial of α over F. We therefore have the following result:

Theorem. *For any irreducible polynomial f over a field F there exists a simple extension $K = F(\alpha)$ of F such that $f(\alpha) = 0$ and f is the minimal polynomial of α.*

2.1.6. Any (not necessarily irreducible) nonconstant polynomial $f \in F[x]$ also has a root in some extension of F: indeed, it suffices to adjoin a root α of one of the irreducible factors of f, then $f(\alpha) = 0$.

2.1.7. It follows that two nonconstant polynomials $f_1, f_2 \in F[x]$ are coprime iff they have a common root in no extension of F. Indeed, if f_1 and f_2 have a common root α, then they both are divisible by the minimal polynomial $m_{\alpha,F}$ of α over F. Conversely, if f_1 and f_2 are not coprime, they have a common irreducible divisor $g \in F[x]$, and a root of g (which exists in some extension of F) is a common root of f_1 and f_2.

2.1.8. Let K/F be an extension. Two algebraic over F elements $\alpha_1, \alpha_2 \in K$ are said to be *conjugate over F* if they are roots of the same irreducible polynomial $p \in F[x]$, that is, if $m_{\alpha_1,F} = m_{\alpha_2,F}$.

Since $m_{\alpha,F}$ has at most $\deg m_{\alpha,F} = \deg_F \alpha$ roots in K, an algebraic over F element $\alpha \in K$ has at most $\deg_F \alpha$ conjugates in K, counting itself.

2.1.9. If L/F is a subextension of an extension K/F, then for any element $\alpha \in K$ algebraic over F we have $m_{\alpha,L} \,\big|\, m_{\alpha,F}$. Hence, the set of conjugates of α over L is a subset of the set of conjugates of α over F.

2.2. The splitting field of a polynomial

2.2.1. If $\varphi\colon F_1 \longrightarrow F_2$ is a homomorphism of fields, then φ naturally extends, by putting $\varphi(x) = x$, to a homomorphism $F_1[x] \longrightarrow F_2[x]$ of the rings of polynomials over F_1 and F_2. We will use this constantly.

2.2.2. We will need the following theorem, which is an obvious generalization of the theorem saying that conjugate elements generate isomorphic extensions.

Theorem. *Let $\varphi\colon F_1 \longrightarrow F_2$ be an isomorphism of two fields, let f_1 be an irreducible polynomial over F_1, let $f_2 = \varphi(f_1)$, let α_1 be a root of f_1 and α_2 be a root of f_2. Then φ extends to an isomorphism $F_1(\alpha_1) \longrightarrow F_2(\alpha_2)$ that maps α_1 to α_2:*

$$\begin{array}{ccc} \varphi\colon F_1(\alpha_1) & \xrightarrow{\sim} & F_2(\alpha_2), \quad \alpha_1 \leftrightarrow \alpha_2. \\ | & & | \\ \varphi\colon F_1 & \xrightarrow{\sim} & F_2 \end{array}$$

Conversely, if $\varphi\colon K_1 \longrightarrow K_2$ is a homomorphism of fields, F_1 is a subfield of K_1, $F_2 = \varphi(F_1)$, and $\alpha_1 \in K_1$ is algebraic over F_1, then $\alpha_2 = \varphi(\alpha_1) \in F_2$ is algebraic over F_2 and $m_{\alpha_2,F_2} = \varphi(m_{\alpha_1,F_1})$.

Indeed, if F_1 and F_2 are isomorphic, we may simply identify them, thus identify f_1 and f_2 and get an isomorphism $F_1(\alpha_1) \longrightarrow F_2(\alpha_2)$ of extensions.

2.2.3. Let K be a field, and let $f \in K[x]$ be a nonconstant. We say that f *completely splits in* K if $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$ for some $a, \alpha_1, \ldots, \alpha_n \in K$. (Informally, "all roots of f are in K"; more exactly, no additional roots of f appear in any extension of K.)

2.2.4. Let F be a field and let $f \in F[x]$ be a nonconstant polynomial. An extension K/F is said to be *a splitting field* of f if this is the minimal extension where f splits completely; that is, f splits completely in K and K is generated by the roots of f: $K = F(\alpha_1, \ldots, \alpha_n)$ such that $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$. (Informally, K is obtained from F by adjoining all roots of f.)

2.2.5. (i) The splittig field of the polynomial $f(x) = x^4 - 5x^2 + 6 = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$ is $\mathbb{Q}\big(\sqrt{2}, \sqrt{3}\big)$.

(ii) The splittig field of the polynomial $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ is $\mathbb{Q}\big(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\big) = \mathbb{Q}\big(\sqrt[3]{2}, \omega\big)$, where $\omega = \frac{-1+\sqrt{-3}}{2} = \sqrt[3]{1}$.

2.2.6. Theorem. *For any field F and any nonconstant polynomial $f \in F[x]$, a splitting field of f exists and is unique up to an isomorphism over F. The degree of this field over F does not exceed* $(\deg f)!$.

Proof of the existing part. The splitting field is obtained by just adjoining the roots of f one-by-one. More formally, we use induction on $n = \deg f$. Let L be the extension of F obtained by adjoining a root α of f, $L = F(\alpha)$. Over L, f factorizes, $f(x) = (x-\alpha)g(x)$, with $g \in L[x]$. By induction, there is a splitting field of g: a field $K = L(\alpha_1, \ldots, \alpha_{n-1})$ such that $g(x) = a(x-\alpha_1)\cdots(x-\alpha_{n-1})$. But then $f(x) = a(x-\alpha)(x-\alpha_1)\cdots(x-\alpha_{n-1})$, so f completely splits in K, and $K = F(\alpha, \alpha_1, \ldots, \alpha_{n-1})$, so K is the splitting field of f. Moreover, we have $[L : F] = \deg_F \alpha \le n$ (since $m_{\alpha,F} \,\big|\, f$), and by induction hypothesis, $[K : L] \le (n-1)!$, so $[K : F] \le n!$. ∎

2.2.7. To prove the uniqueness part of Theorem 2.2.6 by induction, it should be generalized:

Theorem. *Let $\varphi\colon F_1 \longrightarrow F_2$ be an isomorphism of two fields, let $f_1 \in F_1[x]$ and $f_2 = \varphi(f_1)$, and let K_1 and K_2 be a splitting fields of f_1 and f_2 respectively. Then φ extends to an isomorphism $K_1 \longrightarrow K_2$:*

$$\begin{array}{ccc} \varphi\colon K_1 & \xrightarrow{\sim} & K_2 \\ | & & | \\ \varphi\colon F_1 & \xrightarrow{\sim} & F_2 \end{array}$$

which maps the set of roots of f_1 in K_1 onto the set of roots of f_2 in K_2.

Proof. Let p_1 be an irreducible factor of f_1 and let $p_2 = \varphi(p_1)$, then p_2 is an irreducible factor of f_2. Let α_1 be a root of p_1 in K_1 and α_2 be a root of p_2 in K_2, and let $L_1 = F_1(\alpha_1)$, $L_2 = F_2(\alpha_2)$ by Theorem 2.2.2, φ extends to an isomorphism $L_1 \longrightarrow L_2$ with $\varphi(\alpha_1) = \alpha_2$. We now have $f_1(x) = (x-\alpha_1)g_1(x)$ with $g_1 \in L_1[x]$ and $f_2(x) = (x-\alpha_2)g_2(x)$ with $g_2 \in L_2[x]$; since $g_i(x) = f_i(x)/(x-\alpha_i)$, $i = 1, 2$, and $x - \alpha_1 \xrightarrow{\varphi} x - \alpha_2$, we have $\varphi(g_1) = g_2$. Now, K_1 is the splitting field of g_1 and K_2 is the splitting field of g_2; by induction on $\deg f_1 = \deg f_2$, φ extends to an isomoprhism $K_1 \longrightarrow K_2$ which maps the set of roots of g_1 obto the set of roots of g_2. ∎

2.2.8. Let α be an algebraic element over a field F. Then the splitting field K of the minimal polynomial of α "contains all conjugates of α", in the sense that if E is any extension of K, all conjugates of α in E are contained in K.

2.2.9. Given a family $\mathcal{F}$ of polynomials over a field F, *a splitting field of* $\mathcal{F}$ is a minimal extension of F where all polynomials from $\mathcal{F}$ completely split. If $\mathcal{F}$ is finite, $\mathcal{F} = \{f_1, \ldots, f_k\}$, then the splitting field of $\mathcal{F}$ is the splitting field of the single polynomial $f_1 \cdots f_k$. We will prove that the splitting field exists in the case $\mathcal{F}$ is infinite below, after we construct the algebraic closure of F.

2.3. The algebraic closure of a field

2.3.1. A field K is said to be *algebraically closed* if every nonconstant polynomial from $K[x]$ has a root in K. In this case for any $f \in K[x]$ we have $f(x) = (x-\alpha_1)f_1(x) = (x-\alpha_1)(x-\alpha_2)f_2(x) = \cdots = a(x-\alpha_1)\cdots(a-\alpha_n)$, that is, every polynomial from $K[x]$ completely splits in K.

2.3.2. It is *the fundamental theorem of algebra* that $\mathbb{C}$ is algebraically closed.

2.3.3. If K is algebraically closed, then there are no algebraic elements over K, and K has no nontrivial algebraic extensions: indeed, if α is algebraic over K, then $m_{\alpha,K} \in K[x]$ splits in K, so it is linear, and $\alpha \in K$.

2.3.4. Let F be a field; an algebraic extension K/F is called *an algebraic closure* of F if every polynomial from $F[x]$ completely splits in K. An algebraic closure of F is often denoted by $\overline{F}$.

2.3.5. Clearly, if K/F is an extension and K is algebraically closed, then the maximal subextension of K that is algebraic over F is an algebraic closure of F. The converse is also true:

Theorem. *For every field F, the algebraic closure of F is algebraically closed.*

Proof. Let $\overline{F}$ be an algebraic closure of F, and let $f \in \overline{F}[x]$. Let α be a root of f (in some extension of $\overline{F}$); then α is algebraic over $\overline{F}$, which is algebraic over F, so α is algebraic over F. But $m_{\alpha,F}$ completely splits in $\overline{F}$, so $\alpha \in \overline{F}$. ■

2.3.6. An algebraic closure $\overline{F}$ of F is just the splitting field of the set $F[x]$ of all polynomials over F. Indeed, every polynomial from $F[x]$ splits in $\overline{F}$. On the other hand, every element of $\overline{F}$ is algebraic over F, so is a root of some polynomial from $F[x]$; hence, $\overline{F}$ is generated by the roots of polynomials from $F[x]$.

Theorem. *For every field F, the algebraic closure of F exists, and is unique up to isomorphism over F.*

Proof of existence. To adjoin all roots of all polynomials we, of course, need Zorn's lemma: Consider the set of all algebraic extensions of F. The union of any chain of algebraic extensions of F is algebraic as well, thus Zorn's lemma applies and provides us with a maximal algebraic extension K of F. Every polynomial from $F[x]$ (as well as from $K[x]$) splits in K since otherwise we would have a nontrivial algebraic extension of K, which would be an algebraic extension of F strictly larger than K.

Actually, this proof contains a mistake: "the set of all algebraic extensions of F" does not actually exist. To correct it, take a "big" set X containing F, – of cardinality strictly larger than the cardinality of the set of all roots of all polynomials from $F[x]$, – and only consider the extensions of F that are subsets of X. The large cardinality of X guarantees that any algebraic extension L/F does not exhaust X, and so, if L' is a larger extension, a copy of L' can be constructed from elements of X. ■

You can find a different, nice proof of this theorem in the textbook.

2.3.7. The uniqueness of the algebraic closure follows from the following proposition:

Proposition. *If K/F is an extension and K is algebraically closed, then for any algebraic extensions L/F there exists an embedding $L/F \longrightarrow K/F$. More generally: if K is algebraically closed, $\varphi\colon F \longrightarrow K$ is an embedding, and an extension L/F is algebraic, then φ extends to an embedding $L \longrightarrow K$.*

Proof. Let's start with the case L/F is finite. Take any $\alpha \in L \setminus F$. The polynomial $\varphi(m_{\alpha,F})$ splits in K; let $\beta \in K$ be a root of $m_{\alpha,F}$. φ the extends to an isomorphism $F(\alpha) \longrightarrow \varphi(F)(\beta)$ by $\varphi(\alpha) = \beta$, and gives an embedding $F(\alpha) \longrightarrow K$. By induction on $[L:F]$, φ further extends to an embedding $L \longrightarrow K$.

Now consider the general case. Take the family of all embeddings $\psi\colon N \longrightarrow K$ where N is a field with $F \subseteq N \subseteq L$ such that $\psi|_F = \varphi$. Zorn's lemma applies to this family and gives a maximal element $\eta\colon M \longrightarrow K$. If $M \neq L$, take any $\alpha \in L \setminus M$, and then η can be extended to an embedding $M(\alpha) \longrightarrow K$, which contradicts its maximality. Hence, $M = L$. ■

2.3.8. As a corollary, we obtain that every algebraic extension of F can be found in $\overline{F}$.

Theorem. *Every algebraic extension of a field F is isomorphic to a subextension of the algebraic closure $\overline{F}$ of F.*

2.3.9. Proof of uniqueness of the algebraic closure. Let K_1 and K_2 be two algeraic closures of F. By Theorem 2.3.8, there is an embedding $\varphi\colon K_1/F \longrightarrow K_2/F$. Now, K_2 is an alebraic extension of $\varphi(K_1)$, which is isomorphic to K_1 and is therefore algebraically closed; hence, $K_2 = \varphi(K_1)$, thus φ is an isomorphism. ■

2.3.10. We now have:

Theorem. *For any field F and any family $\mathcal{F} \subseteq F[x]$ of polynomials a splitting field of $\mathcal{F}$ exists and is unique up to isomorphism.*

Proof. Let K be the subfield of $\overline{F}$ generated by all the roots of all the polynomials from $\mathcal{F}$; then K is the splitting field of $\mathcal{F}$. It is clearly the only splitting field of $\mathcal{F}$ contained in $\overline{F}$. Now, any other splitting field of $\mathcal{F}$ has a copy in $\overline{F}$, which must be K. So, all splitting fields of $\mathcal{F}$ are isomorphic (as extensions of F). ■

2.3.11. (i) The algebraic closure of $\mathbb{R}$ is $\mathbb{C}$.

(ii) The algebraic closure of $\mathbb{Q}$ is not $\mathbb{C}$ (since $\mathbb{C}$ is not algebraic over $\mathbb{Q}$), it is the field of all complex algebraic numbers.

2.4. Separable and inseparable polynomials and extensions

2.4.1. Let F be a field. A nonconstant polynomial $f \in F[x]$ is said to be *separable* if it has no multiple roots in its splitting field (and so, in any extension of F), and *inseparable* otherwise.

A polynomial f of degree $n \geq 1$ is separable iff f has n distinct roots in its splitting field.

2.4.2. As we know, a root α of a polynomial f is a multiple root of f iff it is a root of the derivative f' of f as well. Thus, a polynomial f is separable iff it has no common roots with its derivative f', that is, iff f and f' are coprime.

2.4.3. Let f be an irreducible polynomial over a field F. Then f and f' must be coprime, unless $f' = 0$. This is impossible if $\operatorname{char} F = 0$; thus, if $\operatorname{char} F = 0$, every irreducible polynomial over K is separable. But if $\operatorname{char} F = p \neq 0$, this is possible: an irreducible polynomial f is inseparable iff it has form $f(x) = a_n x^{np} + a_{n-1}x^{(n-1)p} + \cdots + a_1 x^p + a_0$, that is, if $f(x) = g(x^p)$ for some $g \in F[x]$.

2.4.4. An element α algebraic over a field F is said to be *separable* over F if the minimal polynomial of α is separable. α is separable iff it has exactly $\deg_F \alpha$ conjugates over F (counting itself) in certain extension of K (in the splitting field of its minimal polynomial).

2.4.5. An extension K/F is said to be *separable* if every $\alpha \in K$ is separable over F.

2.4.6. Non-separable extensions are said to be *inseparable*. An example of a inseparable extension is $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$: the polynomial $x^p - t^p \in \mathbb{F}_p(t^p)[x]$ is irreducible and is the minimal polynomial of $t \in \mathbb{F}_p(t)$, but is inseparable – it has a single root t of multiplicity p.

2.4.7. Theorem. *If K/F is a separable extension, then for any subextension L/F of K/F, both L/F and K/L are separable.*

(The converse of this theorem is also true, but we cannot prove it yet.)

Proof. Any $\alpha \in L$ is also in K, and so is separable over F.

For any $\alpha \in K$, we have $m_{\alpha,L} \,\big|\, m_{\alpha,F}$, and since $m_{\alpha,F}$ is separable, $m_{\alpha,L}$ is separable too, so α is seprable over L. ■

2.4.8. A field F is said to be *perfect* if every algebraic extension of F is separable.

2.4.9. Theorem. *Any field of characteristic zero is perfect. A field F of characteristic p is perfect iff for every $a \in F$, $\sqrt[p]{a} \in F$ as well (that is, there exists $b \in F$ such that $b^p = a$).*

Proof. In characteristic zero, every irreducible polynomial is separable.

Let $\operatorname{char} F = p$. Assume that for every $a \in F$, $\sqrt[p]{a} \in F$. Let $f \in F[x]$ be an irreducible inseparable polynomial, $f(x) = a_n x^{np} + a_{n-1}x^{(n-1)p} + \cdots + a_1 x^p + a_0$. For each i, find $b_i \in F$ such that $b_i^p = a_i$, and put $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$. Then $f(x) = b_n^p x^{np} + b_{n-1}^p x^{(n-1)p} + \cdots + b_1^p x^p + b_0^p = g(x)^p$, so f cannot be irreducible.

Converely, assume that there is $a \in F$ such that $\sqrt[p]{a}$ is not in F. Then the polynomial $f(x) = x^p - a$ is inseparable; let's show it is irreducible. Adjoin a root α of f, that is, an element α such that $\alpha^p = a$; then $f(x) = x^p - \alpha^p = (x-\alpha)^p$. If f is reducible, let $h \in F[x]$ be an irreducible factor of f. Then $h(x) = (x-\alpha)^k$

for some $1 \le k \le p-1$. Since $\alpha \notin F$, we actually have $2 \le k \le p-1$; but then h is irreducible, has a multiple root, and is not of the form $h(x) = g(x^p)$ for some $g \in F[x]$, contradiction. ■

2.4.10. Let F be a field of characteristic p. The mapping $\phi\colon F \longrightarrow F$ defined by $\phi(a) = a^p$ is an endomorphism of F: for any $a, b \in F$, $\phi(a+b) = (a+b)^p = a^p + b^p = \phi(a) + \phi(b)$, and $\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$. ϕ is called *the Frobenius endomorphism* of F.

2.4.11. By Theorem 2.4.9, F is a perfect field iff its Frobenius endomorphism is surjective, that is, is an automorphism.

2.4.12. If F is a finite field, then its Frobenius endomorphism, being injective (as every (nonzero) field homomorphism), is also surjective. So, every finite field is perfect.

2.4.13. The field $F = \mathbb{F}_p(t)$ of rational functions over the field $\mathbb{F}_p$ is non-perfect: indeed, the polynomial $f(x) = x^p - t \in F[x]$ is irreducible, but $f' = 0$. (f has a single root $\alpha = \sqrt[p]{t}$ of multiplicity p: indeed, $f(x) = (x-\alpha)^p$.)

---

3. Cyclotomic extensions and finite fields

3.1. Roots of unity and cyclotomic fields

Let F be a field.

3.1.1. For every $n \in \mathbb{N}$, the elements a of F satisfying $a^n = 1$ are called *the nth roots of unity* or *roots of unity of degree n* in F; these are the roots of the polynomial $x^n - 1$. The nth roots of unity which are not dth roots of unity for $d < n$ are called *primitive nth roots of unity*. Every root of unity of degree $d \,\big|\, n$ is an nth root of unity, and every nth root of unity is a primitive dth roots of unity for some $d \,\big|\, n$.

3.1.2. Lemma. *Any finite subgroup of the multiplicative group of a field is cyclic.*

Proof. Let G be a finite group of elements of a field F under multiplication, let $|G| = m$. Let k be the senior invariant factor of G, so that $a^k = 1$ for all $a \in G$. This means that the polynomial $x^k - 1$ has $\ge m$ roots in F, so $k \ge m$. Hence, $k = m$ and G has a unique cyclic component, that is, is cyclic. ■

Thus, the nth roots of unity form, under multiplication, a cyclic group. Since $a^n = 1$ for all elements of this group, the order of the group divides n.

3.1.3. The splitting field of the polynomial $x^n - 1 \in F[x]$ is called *the nth cyclotomic extension* of F; the n-th cyclotomic extension of $\mathbb{Q}$ is called *the nth cyclotomic field*.

3.1.4. Let K be the nth cyclotomic extension of F, and let G_n be the group of roots of unity of degree n in K. If $\operatorname{char} F = 0$ or $\operatorname{char} F = p$ with $p \nmid n$, then the polynomial $x^n - 1$ is separable (it has no common roots with its derivative nx^{n-1}), so $|G_n| = n$.

If $\operatorname{char} F = p$ and $n = p^r m$, $(m, p) = 1$, then the roots of unity of degree n are the roots of unity of degree m: $a^{p^r m} = 1$ implies that $\phi^r(a^m) = (a^m)^{p^r} = 1$ where ϕ is the Frobenius endomorphism, and so $a^m = 1$. Hence, $|G_n| = m$.

3.1.5. From now on, let us assume that either $\operatorname{char} F = 0$ or $\operatorname{char} F \nmid n$. Then $x^n - 1$ is separable, $|G_n| = n$, and the set of primitive nth roots of unity in K is the set of elements generating G_n. If ω is a primitive nth root of unity, then the nth roots of unity are ω^k, $k = 0, 1, \ldots, n-1$; thus, we have $K = F(\omega)$. The primitive nth roots of unity are the elements ω^k with k coprime with n; there are exactly $\varphi(n)$ of them, where φ is Euler's totient function.

3.1.6. The nth roots of unity over $\mathbb{Q}$ are the complex numbers $e^{2k\pi i/n}$, $k = 0, 1, \ldots, n-1$. $\omega = e^{2\pi i/n}$ is a primitive nth root of unity.

3.1.7. Let P_n be the set of primitive nth roots of unity over F (contained in the cyclotomic extension of F): $P_n = \left\{\omega^k : 1 \le k \le n-1,\ (k, n) = 1\right\}$, where ω is any primitive nth root of unity. The polynomial $\Phi_n(x) = \prod_{\alpha \in P_n}(x - \alpha)$ is called *the nth cyclotomic polynomial*. Φ_n is monic, separable, and has degree $\varphi(n)$.

3.1.8. Theorem. *For every $n \in \mathbb{N}$, $\prod_{d|n} \Phi_d(x) = x^n - 1$.*

Proof. We have

$$x^n - 1 = \prod_{\omega:\omega^n=1} (x - \omega) = \prod_{d|n} \prod_{\alpha \in P_d} (x - \alpha) = \prod_{d|n} \Phi_d(x).$$

■

3.1.9. Corollary. *For every $n \in \mathbb{N}$, the coefficients of Φ_n are in the prime subfield. In characteristic zero, $\Phi_n \in \mathbb{Z}[x]$ (has integer coefficients).*

Proof. If by induction, for all $d < n$, Φ_d have their coefficients in the prime subfield, then so is $\Phi_n(x) = (x^n-1)/\prod_{\substack{d|n \\ d<n}} \Phi_d(x)$. If, in characteristic zero, the coefficients of Φ_d are in $\mathbb{Z}$, then since they are all monic, the coefficients of Φ_n are in $\mathbb{Z}$ by Gauss's lemma. ■

3.1.10. The formula $\Phi_n(x) = (x^n - 1)/\prod_{\substack{d|n \\ d<n}} \Phi_d(x)$ allows us to compute the cyclotomic polynomials inductively. We have $\Phi_1(x) = x-1$, $\Phi_2(x) = (x^2-1)/(x-1) = x+1$, $\Phi_3(x) = (x^3-1)/(x-1) = x^2+x+1$, $\Phi_4 = (x^4-1)/(x-1)(x+1) = x^2+1$.

Here are the initial cyclotomic polynomials:

$$\begin{aligned}
&\Phi_1(x) = x - 1\\
&\Phi_2(x) = x + 1\\
&\Phi_3(x) = x^2 + x + 1\\
&\Phi_4(x) = x^2 + 1 \quad \big(= \Phi_2(x^2)\big)\\
&\Phi_5(x) = x^4 + x^3 + x^2 + x + 1\\
&\Phi_6(x) = x^2 - x + 1 \quad \big(= \Phi_3(-x)\big)\\
&\Phi_7(x) = x^6 + \cdots + x + 1\\
&\Phi_8(x) = x^4 + 1 \quad \big(= \Phi_2(x^4)\big)\\
&\Phi_9(x) = x^6 + x^3 + 1 \quad \big(= \Phi_3(x^3)\big)\\
&\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1 \quad \big(= \Phi_5(-x)\big)\\
&\Phi_{11}(x) = x^{10} + \cdots + x + 1\\
&\Phi_{12}(x) = x^4 - x^2 + 1 \quad \big(= \Phi_6(x^2)\big)
\end{aligned}$$

and

$$\begin{aligned}
&\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1\\
&\Phi_{36}(x) = x^{12} - x^6 + 1 \quad \big(= \Phi_6(x^6) = \Phi_3(-x^6)\big)\\
&\Phi_{105}(x) = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24}\\
&\qquad\qquad - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1
\end{aligned}$$

(Φ_{105} is the first cyclotomic polynomial that has a coefficient distinct from ± 1 or 0. (Notice that $105 = 3{\cdot}5{\cdot}7$.))

3.1.11. The proof of following facts are left as exercises:

(i) For any odd $n \geq 3$, $\Phi_{2n}(x) = \Phi_n(-x)$.

(ii) For any prime p, $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, and for any $r \in \mathbb{N}$, $\Phi_{p^r}(x) = \Phi_p(x^{p^{r-1}})$.

(iii) More generally, if p is prime and $n = mp^r$ with $p \nmid m$, then $\Phi_n(x) = \Phi_{pm}(x^{p^{r-1}})$.

3.1.12. Theorem. *For every $n \in \mathbb{N}$, Φ_n is irreducible in $\mathbb{Q}[x]$. Thus, in characteristic zero, all primitive nth roots of unity are conjugate over $\mathbb{Q}$.*

Proof. By Gauss's lemma, we only need to show that Φ_n is irreducible in $\mathbb{Z}[x]$. Assume that it is reducible, let $\Phi_n = fg$ where $f, g \in \mathbb{Z}[x]$ are nonconstant and monic. Let ω be a primitive root of unity of degree n, then all roots of Φ_n have form ω^k for some k with $(k, n) = 1$; some of them are roots of f and the other are roots of g. There must be k and a prime p, both coprime with n, such that $\alpha = \omega^k$ is a root of f and $\alpha^p = \omega^{kp}$ is a root of g. Then α is a common root of f and $g(x^p)$, so $f(x)$ and $g(x^p)$ are not coprime, and have a common factor. Let $\tilde{f} = f \bmod p \in \mathbb{F}_p[x]$ and $\tilde{g} = g \bmod p \in \mathbb{F}_p[x]$, then $\tilde{f}(x)$ and $\tilde{g}(x^p) = \tilde{g}(x)^p$ have a common factor, so $\tilde{f}$ and $\tilde{g}$ have a common factor, and so $\tilde{\Phi}_n = \tilde{f}\tilde{g}$ is inseparable, contradiction. ■

3.1.13. So, in characteristic zero, for any n, Φ_n is the minimal polynomial of every primitive nth root of unity. We therefore have:

Corollary. *For every $n \in \mathbb{N}$, the nth cyclotomic field has degree $\varphi(n)$ over $\mathbb{Q}$.*

3.2. Finite fields

3.2.1. Any finite field K has p^n elements, where $p = \operatorname{char} K$ and $n = [K : \mathbb{F}_p]$.

3.2.2. Let K be a field of order p^n. Then the multiplicative group K^* of K has $p^n - 1$ elements, so for any nonzero $\alpha \in K$ we have $\alpha^{p^n-1} = 1$, so for all $\alpha \in K$ we have $\alpha^{p^n} = \alpha$. Hence, all p^n elements of K are roots of the polynomial $x^{p^n} - x$, and K is the splitting field of this polynomial.

Conversely, given a prime p and a positive integer n, let K be the splitting field of the polynomial $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. Let S be the set of the roots of f in K. Since $f' \neq 0$, f is separable, so $|S| = p^n$. Next, S is a field: if $\alpha, \beta \in S$, that is, $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$, then $(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta$, $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$, and $(\alpha^{-1})^n = \alpha^{-1}$, so $f(\alpha + \beta) = f(\alpha\beta) = f(\alpha^{-1}) = 0$. Hence, $K = S$, and $|K| = p^n$.

Since the splitting field of any polynomial exists and is unique up to isomorphism, we get:

Theorem. *For every prime p and every $n \in \mathbb{N}$ there exists a unique, up to isomorphism, field of order p^n; it is the splitting field of the polynomial $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$, and consists of the roots of this polynomial.*

The (unique up to isomorphism) field of cardinality $q = p^n$ is denoted by $\mathbb{F}_q$.

3.2.3. Theorem. *For any prime p and every $n \in \mathbb{N}$,*

(i) *the field $\mathbb{F}_{p^n}$ is a simple extension of its prime subfield $\mathbb{F}_p$;*

(ii) *there exists an irreducible polynomial of degree n in $\mathbb{F}_p[x]$.*

Proof. The group $\mathbb{F}_{p^n}^*$ of nonzero elements of $\mathbb{F}_{p^n}$ under multiplication is cyclic; let α be any generator of this group. Then the powers of α run over the set of all nonzero elements of $\mathbb{F}_{p^n}$, so α generates this field, $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$. It also follows that $\deg_{\mathbb{F}_p} \alpha = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, so $m_{\alpha,\mathbb{F}_p} \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree n. ■

3.2.4. Lemma. *If $d, n \in \mathbb{N}$ and $d \,\big|\, n$, then $(x^d - 1) \,\big|\, (x^n - 1)$ and for any $r \in \mathbb{N}$, $(x^{r^d-1} - 1) \,\big|\, (x^{r^n-1} - 1)$.*

Proof. $x^n - 1 = (x^d)^{n/d} - 1 = (x^d - 1)\big((x^d)^{n/d-1} + \cdots + x^d + 1\big)$, so $(x^d - 1) \,\big|\, (x^n - 1)$. It follows that for any $r \in \mathbb{N}$, $(r^d - 1) \,\big|\, (r^n - 1)$, so now $(x^{r^d-1} - 1) \,\big|\, (x^{r^n-1} - 1)$. ■

3.2.5. Theorem. *For any prime p and $n \in \mathbb{N}$, the field $\mathbb{F}_{p^n}$ contains a single copy of the field $\mathbb{F}_{p^d}$ for each d dividing n, and has no other subfields.*

It follows that the diagram of subextensions of $\mathbb{F}_{p^n}$ looks exactly like the diagram of subgroups of $\mathbb{Z}_n$.

Proof. Let L be a subfield of $\mathbb{F}_{p^n}$ of degree d over $\mathbb{F}_p$. Then d divides $n = \big|\mathbb{F}_{p^n} : \mathbb{F}_p\big|$. Thus, $|L| = p^d$ and $L \cong \mathbb{F}_{p^d}$. Hence, all elements $\alpha \in L$ are roots of the polynomial $x^{p^d} - x$; since there are at most p^d such roots in $\mathbb{F}_{p^n}$, there may be at most one such subfield L of $\mathbb{F}_{p^n}$.

On the other hand, for every $d \,\big|\, n$ the polynomial $x^{p^d-1} - 1$ divides $x^{p^n-1} - 1$, thus all roots of $x^{p^d-1} - 1$, which are just all nonzero elements of $\mathbb{F}_{p^d}$, are contained in $\mathbb{F}_{p^n}$. ■

3.2.6. The following theorem allows to find inductively the number of irreducible polynomials of degree n in $\mathbb{F}_p[x]$.

Theorem. *If $\psi(n)$ is the number of monic irreducible polynomials of degree n in $\mathbb{F}_p[x]$, then $\sum_{d|n} d\psi(d) = p^n$.*

Proof. For every d dividing n let P_d be the set of monic irreducible polynomials from $\mathbb{F}_p[x]$ of degree d. Every element of $\mathbb{F}_{p^n}$ is a root of the polynomial $f = m_{\alpha,\mathbb{F}_p}$ from P_d for some $d \,\big|\, n$; on the other hand, for every $d \,\big|\, n$, every $f \in P_d$ is separable and splits completely in $\mathbb{F}_{p^d}$ and so in $\mathbb{F}_{p^n}$. So, $\prod_{d|n} \prod_{f \in P_d} f(x) = \prod_{\alpha \in \mathbb{F}_{p^n}} (x - \alpha) = x^{p^n} - x$, and $\sum_{d|n} d\psi(d) = p^n$. ■

3.2.7. For any prime p, the fileds $\mathbb{F}_{p^{n!}}$, $n \in \mathbb{N}$, form a nested sequence, $\mathbb{F}_p \subseteq \mathbb{F}_{p^{2!}} \subseteq \mathbb{F}_{p^{3!}} \subseteq \mathbb{F}_{p^{4!}} \subseteq \cdots$. The union of this sequence, $\overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^{n!}}$, is an algebraic extension of $\mathbb{F}_p$ that contains all roots of all irreducible polynomials from $\mathbb{F}_p$; hence, it is the algebraic closure of $\mathbb{F}_p$.

---

4. Galois extensions and the Galois theorem

4.1. Embeddings of an extension and conjugate subextensions

This section may be cumbersome, but it is a key to the Galois theory.

4.1.1. Let K/F and E/F be two extensions. A (nonzero, of course) homomorphism $K/F \longrightarrow E/F$ (that is, a homomorphism $K \longrightarrow E$ which is identical on F) is called *an embedding of K/F to E/F*, or *an embedding of K into E over F*.

4.1.2. An isomorphism $K/F \longrightarrow K/F$ is called *an automorphism* of K/F, or *an automorphism of K over F*. The automorphisms of an extension K/F form a group, denoted by $\mathrm{Aut}(K/F)$.

4.1.3. Let φ be an embedding of an extension K/F into an extension E/F. Then for any polynomial $f \in F[x]$, $\varphi(f) = f$ (since φ preserves the coefficients of f). So, for any root α of f in K, $\varphi(\alpha)$ is a root of f in E: $f(\varphi(\alpha)) = \varphi(f)(\varphi(\alpha)) = \varphi(f(\alpha)) = \varphi(0) = 0$.

In particular, if K/F is a subextension of E/F, then any embedding of K/F into E/F maps every element $\alpha \in K$ algebraic over F to a root of the minimal polynomial of α, that is, to a conjugate to α over F.

4.1.4. If K/F is an algebraic extension, then any embedding $\varphi\colon K/F \longrightarrow K/F$ is an automorphism of K/F. Indeed, if K/F is finite, then φ must be surjective, so is an automorphism. In the general case, to show that φ is surjective, let $\alpha \in K$, and let L be the subfiled of K generated by the conjugates of α in K. Since φ permutes the roots of $m_{\alpha,F}$, we have $\varphi(L) \subseteq L$, and since L/F is finite, $\varphi(L) = L$. So, $\alpha \in \varphi(L) \subseteq \varphi(K)$.

4.1.5. Let E/F be an extension, and let α be an element algebraic over F. The set of embeddings $F(\alpha)/F \longrightarrow E/F$ is in one-to-one correspondence with the set of roots of the minimal polynomial $m_{\alpha,F}$ of α in E: each embedding $\varphi\colon F(\alpha)/F \longrightarrow E/F$ is defined by $\varphi(\alpha)$, which must be a root of $m_{\alpha,F}$. There are at most $\deg_F \alpha$ embeddings of $F(\alpha)/F$ into E/F; there are exactly $\deg_F \alpha$ embeddings of $F(\alpha)/F$ into E/F iff $m_{\alpha,F}$ is separable and completely splits in E.

4.1.6. We will need a generalization of 4.1.5: Let $\varphi\colon F_1 \longrightarrow E$ be a homomorphism of fields, let $F_2 = \varphi(F_1)$, let α be an element algebraic over F_1, let $f_1 = m_{\alpha,F_1}$ and let $f_2 = \varphi(f_1) \in F_2[x]$. For any homomorphism $\psi\colon F_1(\alpha) \longrightarrow E$ extending φ (that is, with $\psi|_{F_1} = \varphi$), we have $0 = \psi(f_1(\alpha)) = \varphi(f_1)(\psi(\alpha)) = f_2(\psi(\alpha))$, so ψ maps α to a root α' of f_2, and is defined by α'. Thus, the set of homomorphisms $\psi\colon F_1(\alpha) \longrightarrow E$ extending φ is in one-to-one correspondence with the set of roots of f_2 in E. There are at most $\deg f_2 = \deg f_1 = \deg_{F_1} \alpha$ such homomorphisms of F_1 to E; there are exacly $\deg_{F_1} \alpha$ such homomorphisms iff f_2 is separable and completely splits in E.

Note also that if φ is a homomorphism over a subfield F of F_1 and F_2 (that is, with $\varphi|_F = \mathrm{Id}_F$) and $f = m_{\alpha,F}$, then $f_1 \,|\, f$, and so $f_2 = \varphi(f_1) \,|\, \varphi(f) = f$. So, if f completely splits in E, then f_2 has roots in E, and so, there is an embedding $\psi\colon F_1(\alpha) \longrightarrow E$ extending φ.

4.1.7. Theorem. *Let E/F be an extension, let K/F be a finite extension, let $n = [K : F]$. Then there are at most n embeddings $K/F \longrightarrow E/F$. There are exactly n embeddings $K/F \longrightarrow E/F$ iff K/F is separable and for every $\alpha \in K$, $m_{\alpha,F}$ completely splits in E. For this, it suffices if there is a set of generators $\{\alpha_1, \ldots, \alpha_k\}$ of K/F such that for each i, $m_{\alpha_i,F}$ is separable and completely splits in E.*

Proof. Represent K as a tower of simple extensions, $K = L_k/L_{k-1}/\cdots/L_1/L_0 = F$, where for each i, $L_i = L_{i-1}(\alpha_i)$ for some $\alpha_i \in K$. Then $n = \deg_F \alpha_1 \cdot \deg_{L_1} \alpha_2 \cdots \deg_{L_{k-1}} \alpha_k$. By 4.1.5, there are $\leq \deg_F \alpha_1$ embeddings $L_1/F \longrightarrow E/F$; by 4.1.6, each such embedding has $\leq \deg_F \alpha_2$ extensions to a homomorphism $L_2 \longrightarrow E$; etc., with the total number of embeddings $K/F \longrightarrow E/F$ being $\leq \deg_F \alpha_1 \cdot \deg_{L_1} \alpha_2 \cdots \deg_{L_{k-1}} \alpha_k = n$.

Assume that $K = F(\alpha_1, \ldots, \alpha_k)$ where for each i, α_i has exactly $\deg_F \alpha_i$ conjugates in E, and let $L_0 = F$ and $L_i = L_{i-1}(\alpha_i)$, $i = 1, \ldots, k$. Then there are exactly $\deg_F \alpha_1$ embeddings $L_1/F \longrightarrow E/F$. Let φ be such an embedding. The minimal polynomial m_{α_2,L_1} is an irreducible divisor of $m_{\alpha_2,F}$, and since φ

fixes F, $\varphi(m_{\alpha_2,L_1})$ is also an irreducible divisor of $m_{\alpha_2,F}$, so it is separable and completely splits in E. Thus by 4.1.6, φ has $\deg_{L_1}\alpha_2$ extensions to a homomorphism $L_2 \longrightarrow E$. And so on, with the total number of embeddings $K/F \longrightarrow E/F$ being equal to $\deg_F \alpha_1 \cdot \deg_{L_1}\alpha_2 \cdots \deg_{L_{k-1}}\alpha_k = n$.

If there is an element $\alpha \in K$ for which $m_{\alpha,F}$ has less than $\deg_F \alpha$ roots in E, then in the argument above, put $\alpha = \alpha_1$. We will then get that the total number of embeddings $K/F \longrightarrow E/F$ is less than n. ■

4.1.8. If K/F is a subextension of E/F and $\varphi\colon K/F \longrightarrow E/F$ is an embedding, then the extension $\varphi(K)/F$ is said to be *conjugate* to K/F. By Theorem 4.1.7, a subextension of degree n may have at most n conjugates in an extension E/F.

4.2. Normal extensions

In the textbook the term "normal extension" is not introduced, replaced by "a splitting field". (Indeed, we will see that these two classes of extensions coincide.) But the notion of a normal extension is commonly used, is advantageous, and is closely related to the notion of a normal subgroup, so I prefer to use it.

4.2.1. An algebraic extension K/F is said to be *normal* if for any $\alpha \in K$ "all conjugates of α are in K", that is, the minimal polynomial of α over F completely splits in K. Equivalently, K/F is normal if any irreducible polynomial from $F[x]$ that has a root in K completely splits in K, that is, K is the splitting field of the minimal polynomials of all its elements.

In diagrams, the normality of an extension is indicated by a double line: $\begin{matrix} K \\ \| \\ F \end{matrix}$

4.2.2. The extensions $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ are normal, the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not.

4.2.3. Every quadratic extension is clearly normal.

4.2.4. The following theorem is easy:

Theorem. (i) *If L/F is a subextension of a normal extension K/F, then K/L is also normal.*
(ii) *If L_1 and L_2 are normal subextensions of an extension K/F, then the intersection $(L_1 \cap L_2)/F$ is also normal.*

(Notice that in (i), the subextension L/F does not have to be normal!)

Proof. (i) For any $\alpha \in K$, $m_{\alpha,L} \,\big|\, m_{\alpha,F}$ and $m_{\alpha,F}$ splits completely in K, so $m_{\alpha,L}$ also splits completely.
(ii) For every $\alpha \in L_1 \cap L_2$, $m_{\alpha,F}$ splits completely and all its roots are contained in both L_1 and L_2, so in $L_1 \cap L_2$. ■

4.2.5. Theorem. *If an algebraic extension K/F is normal then for every extension E/K and every embedding $\varphi\colon K/F \longrightarrow E/F$ one has $\varphi(K) \subseteq K$ (and so, φ is an automorphism of K/F). Conversely, if there is an extension E/K such that E/F is normal and for every embedding $\varphi\colon K/F \longrightarrow E/F$ one has $\varphi(K) \subseteq K$, then K/F is normal.*

Proof. Let K/F be normal, E/K be an extension, and $\varphi\colon K/F \longrightarrow E/F$ be an embedding. For any $\alpha \in K$, $\varphi(\alpha)$ is conjugate to α in E, and thus is contained in K. So, $\varphi(K) \subseteq K$.

In the other direction, assume that K/F is not normal, and let $\alpha \in K$ be such that $m_{\alpha,F}$ does not split completely in K. Let $\overline{K}$ be the algebraic closure of K, and let $\beta \in \overline{K}$ be a root of $m_{\alpha,F}$ which is not in K. There is an isomorphism $\varphi\colon F(\alpha) \longrightarrow F(\beta)$ that fixes F and maps α to β, and we can extend φ to an embedding $K \longrightarrow \overline{K}$. Since $\varphi(\alpha) = \beta \notin K$, we have $\varphi(K) \not\subseteq K$. Now, if E is an extension of K such that E/F is normal, we may assume that $E \subseteq \overline{K}$. Then $\varphi(E) = E$, so φ can be seen as an embedding $K/F \longrightarrow E/F$ with $\varphi(K) \not\subseteq K$. ■

4.2.6. Theorem. *Assume that an algebraic extension K/F is generated by a set S such that for every $\alpha \in S$, all conjugates of α over F are in K. (That is, the minimal polynomial of α over F splits in K.) Then K/F is normal. In particular, the splitting field of any family $\mathcal{F} \subseteq F[x]$ is a normal extension of F.*

Proof. For any extension E/K, any embedding $\varphi\colon K/F \longrightarrow E/F$ maps all elements of S to their conjugates, which are in K by assumption. Since S generates K, this implies that $\varphi(K) \subseteq K$. ■

4.2.7. As a corollary, we get:

Theorem. *If L_1 and L_2 are normal subextensions of an extension K/F, then their composite $(L_1L_2)/F$ is also normal.*

4.2.8. Theorem. *For any algebraic extension K/F there exists a normal extension E/F containing K such that no proper subextension of E/F containing K is normal. If K/F is finite, then E/F is also finite.*

This extension E/F is called *the normal closure* of K/F.

Proof. E is just the splitting field of the set of the minimal polynomials of any set of generators of K over F. ■

4.2.9. The following is an important property of normal extensions:

Theorem. *Let K/F be a normal extension and let L/F be its subextension. Then every embedding $L/F \longrightarrow K/F$ extends to an automorphism of K/F.*

Proof. Let E be the algebraic closure of K. Any embedding $\varphi\colon L/F \longrightarrow K/F$, and so $L/F \longrightarrow E/F$, extends to an embedding $\varphi\colon K/F \longrightarrow E/F$. Since K/F is normal, $\varphi(K) = K$. ■

4.3. Galois extensions and Galois groups

4.3.1. Here is the central definition of the course: A finite normal separable extension is called *a Galois extension*.

4.3.2. We have:

Theorem. *A finite extension K/F is Galois iff $|\operatorname{Aut}(K/F)| = [K : F]$.*

Indeed, elements of $\operatorname{Aut}(K/F)$ are just embeddings $K/F \longrightarrow K/F$, and we have exactly $[K : F]$ such embeddings iff K/F is separable and normal.

4.3.3. If K/F is a Galois extension, then the group $\operatorname{Aut}(K/F)$ is called *the Galois group* of K/F, and is denoted by $\operatorname{Gal}(K/F)$. By Theorem 4.3.2, $\operatorname{Gal}(K/F)$ is a finite group of order $[K : F]$.

A Galois extension is called *cyclic*, *abelian*, *nilpotent*, or *solvable*, if its Galois group is cyclic, abelian, nilpotent, or solvable respectfully.

4.3.4. The action of every element of the Galois group $G = \operatorname{Gal}(K/F)$ of a Galois extension K/F is defined by its action on the generators of K/F, which are mapped to some their conjugates. Thus G can be seen as a subgroup of the group of permutations of a finite set of generators and their conjugates.

4.3.5. The action of the Galois group $G = \operatorname{Gal}(K/F)$ of a Galois extension K/F on any set of elements of K conjugate over F is transitive: indeed, if $\alpha, \alpha' \in K$ are conjugate over F, then, by 4.2.9, the isomorphism $F(\alpha)/F \longrightarrow F(\alpha')/F$ that maps α to α' extends to an automorphism of K/F, that is, to an element of G.

4.3.6. For an extension to be Galois, it suffices if it is "Galois on generators":

Theorem. (i) *A finite extension K/F is Galois iff it is generated by elements separable over F whose all conjugates over F are contained in K.*

(ii) *An extension K/F is Galois iff K is a splitting field of a separable polynomial from $F[x]$.*

4.3.7. If K is the splitting field of a separable polynomial $f \in F[x]$, then the Galois group $\operatorname{Gal}(K/F)$ is also called *the Galois group of f*, and is denoted by $\operatorname{Gal}(f/F)$ or just $\operatorname{Gal}(f)$. Via its action on the roots of f, the group $\operatorname{Gal}(f)$ is (isomorphic to) a subgroup of S_n for $n = \deg f$.

If f is irreducible over F, then, by 4.3.5, $\operatorname{Gal}(f/F)$ acts transitively on the set of the roots of f.

4.3.8. From the definition, the criteria above, and properties of normal and separable extensions we have:

Theorem. (i) *If L/F is a subextension of a Galois extension K/F, then K/L is also Galois.*

(ii) *If L_1 and L_2 are Galois subextensions of an extension K/F, then their intersection $(L_1 \cap L_2)/F$ is also Galois.*

(iii) *If L_1 and L_2 are Galois subextensions of an extension K/F, then their composite $(L_1L_2)/F$ is also Galois.*

4.3.9. If K/F is a finite separable extension, then its normal closure is a Galois extension: indeed, the normal closure of K/F is generated by conjugates of separable elements, which all are also separable. It is called *the Galois closure* of K/F.

The Galois closure of K/F is generated by the conjugates of K over F.

4.4. Composites and towers of separable extensions

Taking the normal closure of a finite separable extension converts it into a Galois extension; we may now use this to obtain the properties of separable extensions that we were not able to prove before.

4.4.1. Theorem. *If an algebraic extension K/F is generated by a set of elements separable over F, then K/F is separable.*

Proof. Let $\alpha \in K$; we need to show that α is separable over F, and for this end we may replace K by a subfield generated by finitely many of the (separable) generators of K/F, and thus assume that K/F is finite. Let E/F be the Galois closure of K/F; then E/F is separable, so K/F is separable. ■

4.4.2. Corollary. *If L_1/F and L_2/F are separable subextensions of an extension K/F, then their composite $(L_1L_2)/F$ is also separable.*

4.4.3. Theorem. *If K/L and L/F are separable extensions, then K/F is separable.*

Proof. Let $\alpha \in K$; we have to prove that α is separable over F, so, we may assume that $K = L(\alpha)$. After replacing L by the field generated by the coefficients of the polynomial $p = m_{\alpha,L}$, we may assume that L/F is finite. Let $n = [L : F]$ and $m = \deg_L \alpha = \deg p$. Let E/F be the normal closure of K/F. Then there are n embeddings $\varphi\colon L/F \longrightarrow E/F$, and every such embedding can be extended to an embedding $K/F \longrightarrow E/F$ by mapping α to a root of $\varphi(p)$. Since p is separable, the polynomial $\varphi(p)$ is also separable; thus there are m extensions of φ to an embedding $K/F \longrightarrow E/F$. So, totally we have $nm = [K : F]$ embeddings $K/F \longrightarrow E/F$, which, by Theorem 4.1.7, implies that K/F is separable. ■

4.4.4. Let K/F be an algebraic extension, let $L/F, L_1/F, L_2/F$ be subextensions of K/F. We have the following:

	finite	separable	normal	Galois
If K is generated by "good" elements then K/F is "good"	−	+	+	−
If K is generated by finitely many "good" elements then K/F is "good"	+	+	+	+
If L_1/F and L_2/F are "good" then $(L_1 \cap L_2)/F$ is "good"	+	+	+	+
If L_1/F and L_2/F are "good" then $(L_1L_2)/F$ is "good"	+	+	+	+
If K/F is "good" then L/F is "good"	+	+	−	−
If K/F is "good" then K/L is "good"	+	+	+	+
If L/F and K/L are "good" then K/F is "good"	+	+	−	−

(Dependently on the column, an element α is assumed to be "good" if, respectively, $\deg_F \alpha < \infty$ (α is algebraic, which is automatic since K/F is algebraic); α is separable; $m_{\alpha,F}$ splits completely in K; and $m_{\alpha,F}$ is separable and splits completely in K. An extension is "good" if it is finite, separable, normal, and Galois respectively.)

4.5. Examples of Galois groups

4.5.1. The Galois group of the polynomial $f(x) = x^2 - 2$ is isomorphic to $\mathbb{Z}_2$: the only nonidentical element of this group maps $\sqrt{2} \mapsto -\sqrt{2}$. (Clearly, the Galois group of any separable quadratic extension is $\mathbb{Z}_2$.)

4.5.2. The Galois group G of the polynomial $f(x) = (x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$ is isomorphic to $V_4 = \mathbb{Z}_2^2$. Namely, $G = \{1, \varphi_1, \varphi_2, \varphi_3\}$, where the action of φ_i on the elements $\sqrt{2}$ and $\sqrt{3}$, generating the splitting field of f, is given by

$$\varphi_1 : \begin{smallmatrix}\sqrt{2}\mapsto -\sqrt{2}\\ \sqrt{3}\mapsto \sqrt{3}\end{smallmatrix}, \qquad \varphi_2 : \begin{smallmatrix}\sqrt{2}\mapsto \sqrt{2}\\ \sqrt{3}\mapsto -\sqrt{3}\end{smallmatrix}, \qquad \varphi_3 : \begin{smallmatrix}\sqrt{2}\mapsto -\sqrt{2}\\ \sqrt{3}\mapsto -\sqrt{3}\end{smallmatrix}.$$

(Clearly, the Galois group of any biquadratic extension in char $\neq 2$ is V_4.)

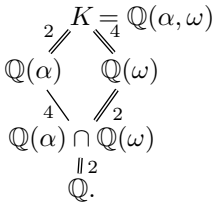
4.5.3. Let $\omega = e^{2\pi i/3}$ and $\alpha = \sqrt[3]{2}$. The Galois group G of the polynomial $f(x) = x^3 - 2$ over $\mathbb{Q}$ has order 6. It acts as a group of all permutations of the roots $\alpha_1 = \alpha$, $\alpha_2 = \omega\alpha$, $\alpha_3 = \omega^2\alpha$ of f, and so, is isomorphic to S_3: $G = \{1, \sigma, \sigma^2, \tau_1, \tau_2, \tau_3\}$ where $\sigma = (\alpha_1, \alpha_2, \alpha_3)$, $\tau_1 = (\alpha_2, \alpha_3)$, $\tau_2 = (\alpha_1, \alpha_3)$, $\tau_3 = (\alpha_1, \alpha_2)$. The action of G on the elements $\omega = e^{2\pi i/3}$ and $\sqrt[3]{2}$, generating the splitting field of f, is given by

$$\sigma : \begin{smallmatrix} \omega \mapsto \omega \\ \alpha \mapsto \omega\alpha \end{smallmatrix}, \qquad \tau_1 : \begin{smallmatrix} \omega \mapsto \omega^2 \\ \alpha \mapsto \alpha \end{smallmatrix}, \qquad \tau_2 : \begin{smallmatrix} \omega \mapsto \omega^2 \\ \alpha \mapsto \omega^2\alpha \end{smallmatrix}, \qquad \tau_3 : \begin{smallmatrix} \omega \mapsto \omega^2 \\ \alpha \mapsto \omega\alpha \end{smallmatrix}.$$

4.5.4. Let ω be a primitive nth root of unity over $\mathbb{Q}$; say, $\omega = e^{2\pi i/n}$. The Galois group G of the cyclotomic extension $\mathbb{Q}(\omega)/\mathbb{Q}$ (and of the nth cyclotomic polynomials Φ_n) has order $\varphi(n)$, where φ is Euler's totient function. Every element of G is uniquely defined by its action on ω, and maps ω to ω^k for some $k \in \mathbb{Z}_n^*$, thus $G = \{\eta_k : k \in \mathbb{Z}_n^*\}$, where $\eta_k(\omega) = \omega^k$. For any $k, l \in \mathbb{Z}_n^*$ we have $\eta_k(\eta_l(\omega)) = \omega^{kl}$, so $\eta_k\eta_l = \eta_{kl}$. Hence, G is isomorphic to $\mathbb{Z}_n^*$.

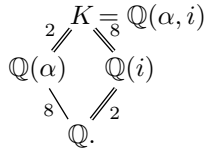
4.5.5. Let L be the nth cyclotomic extension of $\mathbb{Q}$, $L = \mathbb{Q}(\omega)$ where $\omega = e^{2\pi i/n}$. Then the splitting field of the polynomial $f = x^n - 2$ over L is $K = L(\alpha)$ where $\alpha = \sqrt[n]{2}$. Let us assume that $\deg_L(\alpha) = n$ (that is, that $x^n - 2$ is irreducible in $L[x]$), then the Galois group $G = \mathrm{Gal}(f) = \mathrm{Gal}(K/L)$ has order n. Since G acts transitively on the roots of f, there exists $\sigma \in G$ such that $\sigma(\alpha) = \omega\alpha$. Then for any k, $\sigma^k(\alpha) = \omega^k\alpha$, thus σ has order n. So, G is cyclic, isomorphic to $\mathbb{Z}_n$, generated by σ.

4.5.6. Let $K \subset \mathbb{C}$ be the splitting field of the polynomial $f = x^8 - 2 \in \mathbb{Q}[x]$, then $K = (\alpha, \omega)$ where α is the real $\sqrt[8]{2}$ and $\omega = e^{2\pi i/8} = \frac{1+i}{\sqrt{2}}$. Let $G = \mathrm{Gal}(f) = \mathrm{Gal}(K/\mathbb{Q})$. Notice that $\sqrt{2}$ is contained in both $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\omega)$: $\sqrt{2} = \alpha^4$ and $\sqrt{2} = \omega + \omega^7$. Since $\omega \notin \mathbb{Q}(\alpha)$ (ω is not real), $[K : \mathbb{Q}(\alpha)] = 2$. We have the following diagram:



So, $[K : \mathbb{Q}] = 16$.

It is more convenient to use $i = \omega^2$ as a generator instead of ω: since $\omega = \frac{1+i}{\sqrt{2}}$ and $\sqrt{2} \in \mathbb{Q}(\alpha)$, we have $\omega \in \mathbb{Q}(\alpha, i)$, and so, $\mathbb{Q}(\alpha, i) = K$.



Let us find the multiplication in G explicitly. α has 8 conjugates $\alpha\omega^k$, $k = 0, \ldots, 7$, and i has two conjugates $\pm i$, so the total number of choices we have where to send α and i is 16; since $|G| = [K : \mathbb{Q}] = 16$ as well, any choice of the image of α and, independently, of i gives rise to an element of G. Define $\varphi \in G$ by $\varphi(\alpha) = \alpha\omega$, $\varphi(i) = i$, and $\psi \in G$ by $\psi(\alpha) = \alpha$, $\psi(i) = -i$. Then $\varphi(\sqrt{2}) = \varphi(\alpha^4) = \alpha^4\omega^4 = -\sqrt{2}$, so $\varphi(\omega) = -\omega = \omega^5$. So, under the action of φ, we have

$$\alpha \mapsto \alpha\omega \mapsto \alpha\omega^6 \mapsto \alpha\omega^7 \mapsto \alpha\omega^4 \mapsto \alpha\omega^5 \mapsto \alpha\omega^2 \mapsto \alpha\omega^3 \mapsto \alpha \quad \text{and} \quad i \mapsto i,$$

which means that the order of φ in G is 8. The order of ψ is clearly equal to 2. Next, $\psi(\sqrt{2}) = \psi(\alpha^4) = \alpha^4 = \sqrt{2}$, so $\psi(\omega) = \frac{1-i}{\sqrt{2}} = \omega^7$. Hence,

$$(\psi\varphi\psi^{-1})(\alpha) = (\psi\varphi)(\alpha) = \psi(\alpha\omega) = \alpha\omega^7$$

and $(\psi\varphi\psi^{-1})(i) = i$, so $\psi\varphi\psi^{-1} = \varphi^3$. Hence, $G = \langle \varphi, \psi \mid \varphi^8 = \psi^2 = 1,\ \psi\varphi\psi^{-1} = \varphi^3 \rangle$. This is *the semidihedral* (or *the quasidihedral*) group SD_{16}, a semidirect product $Z_8 \rtimes \mathbb{Z}_2$. (There are no other relations in G since $|G| = 16$.)

4.5.7. Let F be a field with $\operatorname{char} F \neq 2$ and let $f \in F[x]$ be an irreducible biquadratic polynomial, $f = x^4 + ax^2 + b$. The roots of f are $\pm\alpha$, $\pm\beta$ where $\alpha = \sqrt{\frac{1}{2}\bigl(-a + \sqrt{a^2 - 4b}\bigr)}$ and $\beta = \sqrt{\frac{1}{2}\bigl(-a - \sqrt{a^2 - 4b}\bigr)}$, with $\alpha\beta = \sqrt{b}$. Since f is irreducible, $\deg_F \alpha = \deg_F \beta = 4$. Let K be the splitting field of f, $K = F(\alpha, \beta) = F(\alpha, \sqrt{b})$, Since f is irreducible, $\delta = \sqrt{a^2 - 4b} \notin F$, and so $[F(\delta) : F] = 2$. We therefore have the extensions diagram

$$\begin{array}{ccc} & K = F(\alpha,\beta) & \\ {\scriptstyle x}\diagup\!\!\diagup & & \diagdown\!\!\diagdown{\scriptstyle x} \\ F(\alpha) & & F(\beta) \\ {\scriptstyle 2}\diagdown\!\!\diagdown & & \diagup\!\!\diagup{\scriptstyle 2} \\ & F(\delta) & \\ & \|{\scriptstyle 2} & \\ & F, & \end{array}$$

where $x = 1$ or 2, so either $[K : F] = 4$ or $[K : F] = 8$.

Let $G = \operatorname{Gal}(f) = \operatorname{Gal}(K/F)$; then G is a subgroup of S_4 of order 4 or 8 that acts transitively on the set $R = \{\alpha, -\alpha, \beta, -\beta\}$. Any element $\varphi \in G$ acts on the square

$$\begin{array}{ccc} \alpha & - & \beta \\ | & & | \\ -\beta & - & -\alpha \end{array}$$

symmetrically with respect to the center of the square: if $\varphi(\lambda) = \gamma$, where $\lambda, \gamma \in \{\pm\alpha, \pm\beta\}$, then $\varphi(-\lambda) = -\gamma$ and $\varphi(\gamma) = \pm\lambda$. So, φ preserves the square, and G is a subgroup of the dihedral group D_8. Since G acts on R transitively, it is isomorphic to one of the groups V_4, $\mathbb{Z}_4$, of D_8.

Assume that $|G| = 4$; this is the case iff $F(\alpha) = F(\beta)$. Since $F(\alpha)$ is a quadratic extension of $F(\delta)$ and both $\alpha^2, \beta^2 \in F(\delta)$, we have that $\beta \in F(\delta)\alpha$, so $\sqrt{b} = \alpha\beta \in F(\delta)\alpha^2 = F(\delta)$; since also $F(\delta)$ is a quadratic extension of F and $\delta^2, \sqrt{b}^2 \in F$, either $\sqrt{b} \in F$ or $\sqrt{b} \in F\delta$. Let $\varphi \in G$ be such that $\varphi(\alpha) = \beta$. We have two options: $\varphi(\beta) = \alpha$ or $\varphi(\beta) = -\alpha$; in the first case φ is a reflection and $G = \{1, \varphi, \psi, \varphi\psi\} \cong V_4$ where $\psi : \alpha \leftrightarrow -\beta$; in the second case φ is a rotation by $\pi/2$ and $G = \{1, \varphi, \varphi^2\varphi^3\} \cong \mathbb{Z}_4$. In the first case, $\varphi(\sqrt{b}) = \varphi(\alpha\beta) = -\beta\alpha = \sqrt{b}$ and $\psi(\sqrt{b}) = \sqrt{b}$, so $\sqrt{b}$ has no conjugates over F except itself, so $\sqrt{b} \in F$; in the second case, $\varphi(\sqrt{b}) = -\sqrt{b}$, so $\sqrt{b} \notin F$.

We obtain: if $\sqrt{b} \in F$ then $G \cong V_4$; if $\sqrt{b}/\delta \in F$, then $G \cong \mathbb{Z}_4$; if both $\sqrt{b}, \sqrt{b}/\delta \notin F$, then $G \cong D_8$.

4.5.8. Let K be a finite field, $K = \mathbb{F}_{p^n}$. The Galois group $G = \operatorname{Gal}\bigl(\mathbb{F}_{p^n}/\mathbb{F}_p\bigr)$ has order $[K : \mathbb{F}_p] = n$. The Frobenius automorphism ϕ of K fixes $\mathbb{F}_p$, thus $\phi \in G$. I claim that the order $|\phi|$ of ϕ is n; this implies that G is cyclic, isomorphic to $\mathbb{Z}_n$, generated by ϕ. Indeed, the multiplictive group of K has a generator α, so that the minimal k for which $\alpha^k = 1$ is $k = p^n - 1$. Thus the minimal m for which $\phi^m(\alpha) = \alpha^{p^m} = \alpha$ is $m = n$, so $|\phi| = n$.

4.6. The fundamental Galois theorem

4.6.1. If K/F be a Galois extension, then for any subextension L/F of K/F, the extension K/L is also Galois, and $\operatorname{Gal}(K/L) \leq \operatorname{Gal}(K/F)$. We therefore have a mapping $L \mapsto \operatorname{Gal}(K/L)$ from the set of subextensions L/F of K/F to the set of subgroups H of G.

4.6.2. Let K be a field a let H be a group of automorphisms of K. An element $\alpha \in K$ is said to be *fixed by* H if $\varphi(\alpha) = \alpha$ for all $\varphi \in H$; a set $S \subseteq K$ is said to be *fixed by* H is all elements of S are fixed by H. By $\operatorname{Fix}(H)$ we denote the set of all elements of K fixed by H; this is a subfield of K, called *the subfield of K fixed by H*.

If K/F is an extension and $H \leq \operatorname{Aut}(K/F)$, then $\operatorname{Fix}(H)$ is an extension of F. We therefore have a mapping $H \mapsto \operatorname{Fix}(H)$ from the set of subgroups H of G to the set of subextensions L/F of K/F.

4.6.3. The fundamental Galois theorem – short version. *Let K/F be a Galois extension and let $G = \operatorname{Gal}(K/F)$. Then the mappings $L \mapsto \operatorname{Gal}(K/L)$ and $H \mapsto \operatorname{Fix}(H)$ are inverses of each other, and define a one-to-one correspondence between the set of subextensions L/F of K/F and the set of subgroups H of G.*

4.6.4. The proof of the Galois theorem is based on the following proposition:

Proposition. *Let K be a field, let G be a finite group of automorphisms of K, and let $F = \operatorname{Fix}(G)$. Then $[K : F] = |G|$.*

(It follows that the extension K/F is Galois.)

Proof. Let $|G| = n$ and $[K : F] = m$; let $G = \{\varphi_1, \dots, \varphi_n\}$ and let $\{\alpha_1, \dots, \alpha_m\}$ be a basis of K over F.
(1) Assume that $n > m$. Consider the following system of m linear equations over K in n variables:

$$\begin{cases} \varphi_1(\alpha_1)x_1 + \cdots + \varphi_n(\alpha_1)x_n = 0 \\ \qquad\qquad \vdots \\ \varphi_1(\alpha_m)x_1 + \cdots + \varphi_n(\alpha_m)x_n = 0. \end{cases}$$

Since $n > m$, this system has a nontrivial solution: there are $\beta_1, \dots, \beta_n \in K$, not all zero, such that

$$\begin{cases} \varphi_1(\alpha_1)\beta_1 + \cdots + \varphi_n(\alpha_1)\beta_n = 0 \\ \qquad\qquad \vdots \\ \varphi_1(\alpha_m)\beta_1 + \cdots + \varphi_n(\alpha_m)\beta_n = 0. \end{cases}$$

For any $(a_1, \dots, a_m) \in F^m$, adding these equalities with coefficients a_i we get

$$\varphi_1\big(\textstyle\sum_{i=1}^m a_i\alpha_i\big)\beta_1 + \cdots + \varphi_n\big(\sum_{i=1}^m a_i\alpha_i\big)\beta_n = 0.$$

But any element α of K is representable in the form $\alpha = \sum_{i=1}^m a_i\alpha_i$ for some $a_1, \dots, a_m \in F$; so, we have $\varphi_1(\alpha)\beta_1 + \cdots + \varphi_n(\alpha)\beta_n = 0$ for all $\alpha \in K$. (That is, we get that φ_i are linearly dependent over K, $\beta_1\varphi_1 + \cdots + \beta_n\varphi_n = 0$.) Choose a minimal such zero linear combination, in the sense of the number of nonzero summands; w.l.o.g. we may assume that this is

$$\varphi_1(\alpha)\beta_1 + \cdots + \varphi_r(\alpha)\beta_r = 0 \tag{A}$$

for all $\alpha \in K$, with $\beta_1, \dots, \beta_r \neq 0$. (Notice that, clearly, $r \geq 2$.)

Now find $\alpha_0 \in K$ for which $\varphi_1(\alpha_0) \neq \varphi_2(\alpha_0)$. For every $\alpha \in K$ we have

$$\varphi_1(\alpha_0\alpha)\beta_1 + \cdots + \varphi_r(\alpha_0\alpha)\beta_r = \varphi_1(\alpha_0)\varphi_1(\alpha)\beta_1 + \cdots + \varphi_r(\alpha_0)\varphi_r(\alpha)\beta_r = 0. \tag{B}$$

Subtracting $\varphi_1(\alpha_0)$(B) from (A) we get

$$\big(\varphi_2(\alpha_0) - \varphi_1(\alpha_0)\big)\varphi_2(\alpha)\beta_1 + \cdots + \big(\varphi_r(\alpha_0) - \varphi_1(\alpha_0)\big)\varphi_r(\alpha)\beta_r = 0$$

for all $\alpha \in K$, which is a nontrivial zero linear combination of φ_i having less than r nonzero summands, contradiction.

(2) Now assume that $m > n$. Consider the following system of n linear equations over K in m variables:

$$\begin{cases} \varphi_1(\alpha_1)x_1 + \cdots + \varphi_1(\alpha_m)x_m = 0 \\ \qquad\qquad \vdots \\ \varphi_n(\alpha_1)x_1 + \cdots + \varphi_n(\alpha_m)x_m = 0. \end{cases}$$

Since $m > n$, this system has a nontrivial solution: there are $\beta_1, \dots, \beta_m \in K$, not all zero, such that

$$\begin{cases} \varphi_1(\alpha_1)\beta_1 + \cdots + \varphi_1(\alpha_m)\beta_m = 0 \\ \qquad\qquad \vdots \\ \varphi_n(\alpha_1)\beta_1 + \cdots + \varphi_n(\alpha_m)\beta_m = 0. \end{cases}$$

This means that for every $\varphi \in G$, $\varphi(\alpha_1)\beta_1 + \cdots + \varphi(\alpha_m)\beta_m = 0$. Choose a minimal such zero linear combination, in the sense of the number of nonzero summands; w.l.o.g. we may assume that this is

$$\varphi(\alpha_1)\beta_1 + \cdots + \varphi(\alpha_r)\beta_r = 0 \tag{C}$$

for all $\varphi \in G$, with $\beta_1, \dots, \beta_r \neq 0$. (Notice that, clearly, $r \geq 2$.)

After dividing (C) by β_1 we may assume that $\beta_1 = 1 \in F$, so $\psi(\beta_1) = \beta_1$ for all $\psi \in G$. It cannot be that all β_i are in F, since we have $\alpha_1\beta_1 + \dots + \alpha_r\beta_r = 0$ (using $\varphi = 1$), and α_i are linearly independent over F; w.l.o.g. assume that $\beta_2 \notin F$. Find $\psi \in G$ such that $\psi(\beta_2) \neq \beta_2$. Applying ψ to (C), we get

$$\psi\big(\varphi(\alpha_1)\beta_1 + \dots + \varphi(\alpha_r)\beta_r\big) = \psi(\varphi(\alpha_1))\psi(\beta_1) + \dots + \psi(\varphi(\alpha_r))\psi(\beta_r) = 0.$$

Since the products $\psi\varphi$ for $\varphi \in G$ run over all elements of G, we have that

$$\varphi(\alpha_1)\psi(\beta_1) + \dots + \varphi(\alpha_r)\psi(\beta_r) = 0 \tag{D}$$

for all $\varphi \in G$. Subtracting (D) from (C) (and recalling that $\psi(\beta_1) = \beta_1$) we get

$$\varphi(\alpha_2)\big(\beta_2 - \psi(\beta_2)\big) + \dots + \varphi(\alpha_r)\big(\beta_r - \psi(\beta_r)\big) = 0$$

for all $\varphi \in G$, which is a nontrivial zero linear combination having less than r nonzero summands, contradiction. ■

4.6.5. Proof of the Galois theorem. Let L/F be a subextension of K/F, let $H = \mathrm{Gal}(K/L)$, and let $\widetilde{L} = \mathrm{Fix}(H)$. Since H fixes L we have $L \subseteq \widetilde{L}$. Let $[K : L] = n$, then $|H| = n$, and by Proposition 4.6.4, $[K : \widetilde{L}] = n$; so, $\widetilde{L} = L$.

Now let H be a subgroup of G, let $L = \mathrm{Fix}(H)$, and let $\widetilde{H} = \mathrm{Gal}(K/L)$. Since H fixes L, we have $H \leq \widetilde{H}$. Let $|H| = n$, then by Proposition 4.6.4, $[K : L] = n$, and $|\widetilde{H}| = n$ since K/L is Galois; so, $\widetilde{H} = H$. ■

4.6.6. The fundamental Galois theorem – full version. *Let K/F be a Galois extension and let $G = \mathrm{Gal}(K/F)$. Let L, L_1 and L_2 be subextensions of K/F and let H, H_1 and H_2 be the corresponding subgroups of G (under the bijection $L \mapsto \mathrm{Gal}(K/L)$). Then*

(i) *$|H| = [K : L]$ and $|G : H| = [L : F]$.*

(ii) *$L_1 \subseteq L_2$ iff $H_1 \geq H_2$, and in this case, $[L_2 : L_1] = |H_1 : H_2|$. So, the diagram of subextensions of K/L is isomorphic to the diagram of subgroups of G flipped upside down.*

(iii) *The subgroup $H_1 \cap H_2$ corresponds to the composite L_1L_2 and the subgroup $\langle H_1, H_2\rangle$ corresponds to the intersection $L_1 \cap L_2$.*

(iv) *Every embedding of L/F into K/F is defined by an element of G; the set of embeddings of L/F into K/F is in a one-to-one correspondence with the set G/H of left cosets of H in G.*

(v) *For any $\varphi \in G$, the subgroup of G corresponding to the conjugate $\varphi(L)$ of L is the conjugate $\varphi H \varphi^{-1}$ of H. The number of conjugates of L/F in K/F equals $|G : N_G(H)|$, where $N_G(H)$ is the normalizer of H in G.*

(vi) *H is a normal subgroup of G iff L/F is a normal extension. In this case, L/F is Galois, the mapping $\varphi \mapsto \varphi|_L$ defines a homomorphism $\mathrm{Gal}(K/F) \longrightarrow \mathrm{Gal}(L/F)$ and induces an isomorphism $G/H \cong \mathrm{Gal}(L/F)$.*

Proof. (i) Since $H = \mathrm{Gal}(K/L)$, we have $|H| = [K : L]$. Now, $|G : H| = |G|/|H| = [K : F]/[K : L] = [L : F]$.

(ii) If $L_1 \subseteq L_2$, then every element of $H_2 = \mathrm{Gal}(K/L_2)$ fixes L_1, so is contained in $H_1 = \mathrm{Gal}(K/L_1)$. Conversely, if $H_2 \leq H_1$, then $L_1 = \mathrm{Fix}(H_1) \subseteq \mathrm{Fix}(H_2) = L_2$. And in this case, $[L_2 : L_1] = [K : L_1]/[K : L_2] = |H_1|/|H_2| = |H_1 : H_2|$. Hence, the diagram of subextensions of K/L is the same as the diagram of subgroups of G, only flipped upside down (and even the numbers near the edges of the diagram, that is, the degrees of subextensions and the indices of subgroups, are the same).

(iii) It follows that for "the minimal diamond" diagram of L_1 and L_2 corresponds to that of H_1 and H_2:

$$\begin{array}{ccc} L_1L_2 & & H_1 \cap H_2 \\ {\scriptstyle n_1}\diagup\ \diagdown{\scriptstyle n_2} & & {\scriptstyle n_1}\diagup\ \diagdown{\scriptstyle n_2} \\ L_1 \quad L_2 & & H_1 \quad H_2 \\ {\scriptstyle m_1}\diagdown\ \diagup{\scriptstyle m_2} & & {\scriptstyle m_1}\diagdown\ \diagup{\scriptstyle m_2} \\ L_1 \cap L_2 & & \langle H_1, H_2\rangle \end{array}$$

so that L_1L_2 (the minimal field containing L_1 and L_2) correspond to $H_1 \cap H_2$ (the maximal subgroup of both H_1 and H_2, and $L_1 \cap L_2$ (the maximal subfield of both L_1 and L_2) correspond to $\langle H_1, H_2\rangle$ (the minimal group containing both H_1 and H_2).

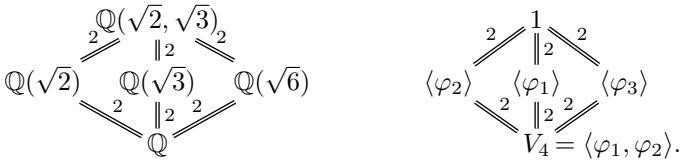
(iv) Since K/F is normal, every embedding $L/F \longrightarrow K/F$ extends to an embedding $K/F \longrightarrow K/F$, that is, an element of G. Two elements φ, ψ of G define the same embedding $L \longrightarrow K$ iff $\varphi^{-1}\psi$ is identical on L, that is, iff $\varphi^{-1}\psi \in \mathrm{Gal}(K/L) = H$, that is, iff $\varphi H = \psi H$.

(v) We have $\psi \in \mathrm{Gal}(K/\varphi(L))$ iff $\psi(\varphi(\alpha)) = \varphi(\alpha)$ for every $\alpha \in L$ iff $\varphi^{-1}\psi\varphi \in \mathrm{Gal}(K/L) = H$. So, $\mathrm{Gal}(K/\varphi(L)) = \varphi H \varphi^{-1}$, a conjugate of H. Thus, the conjugates of L/F are in one-to-one correspondence with the conjugates of H, which, in their turn, are in one-to-one correspondence with left cosets of $N(H)$ in G.

(vi) H is a normal subgroup of G iff it has no conjugates in G but itself, iff L/F has no conjugates in K/F but itself, iff every embedding φ of L/F into K/F preserves L, $\varphi(L) = L$, iff L/F is normal, and so Galois. In this case the mapping $\varphi \mapsto \varphi|_L$ defines a homomorphism $\eta\colon G = \mathrm{Gal}(K/F) \longrightarrow \mathrm{Gal}(L/F)$. Since every automorphism of L/F extends to an automorphism K/F, η is surjective. The kernel of η consists of elements of G that fix L, that is, $\ker(\eta) = \mathrm{Gal}(K/L) = H$. Hence, $\mathrm{Gal}(L/F) \cong G/H$. ∎

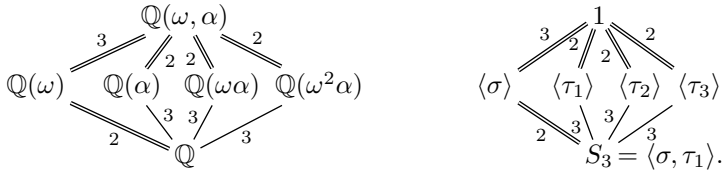
4.7. Examples of diagrams of subextensions and the corresponding Galois groups

4.7.1. The diagram of subextensions of the biquadratic extension $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$, along with the diagram of subgroups of its Galois group:



It follows that $\mathbb{Q}(\sqrt{2},\sqrt{3})$ contains no other subfields!

4.7.2. The diagram of subextensions of the splitting field $K/\mathbb{Q}$ of the polynomial $x^3 - 2$, $K = \mathbb{Q}(\omega, \alpha)$, where $\omega = e^{2\pi i/3}$ and $\alpha = \sqrt[3]{2}$, with the diagram of subgroups of its Galois group:

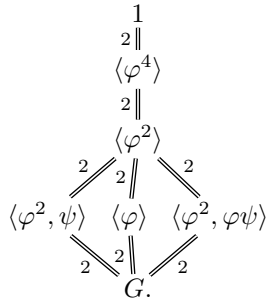


where $\sigma : \left(\begin{smallmatrix}\alpha\mapsto\omega\alpha\\ \omega\mapsto\omega\end{smallmatrix}\right)$ fixes ω, $\tau_1 : \left(\begin{smallmatrix}\alpha\mapsto\alpha\\ \omega\mapsto\omega^2\end{smallmatrix}\right)$ fixes α, $\tau_2 : \left(\begin{smallmatrix}\alpha\mapsto\omega^2\alpha\\ \omega\mapsto\omega^2\end{smallmatrix}\right)$ fixes $\omega\alpha$, and $\tau_3 : \left(\begin{smallmatrix}\alpha\mapsto\omega\alpha\\ \omega\mapsto\omega^2\end{smallmatrix}\right)$ fixes $\omega^2\alpha$. Notice that the subextension $\mathbb{Q}(\omega)/\mathbb{Q}$ is normal (as the corresponding subgroup $\langle\sigma\rangle$), and the subextensions $\mathbb{Q}(\alpha)/\mathbb{Q}$, $\mathbb{Q}(\omega\alpha)/\mathbb{Q}$, $\mathbb{Q}(\omega^2\alpha)/\mathbb{Q}$ are all conjugate (as the corresponding subgroups $\langle\tau_1\rangle$, $\langle\tau_2\rangle$, $\langle\tau_3\rangle$).

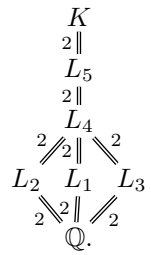
4.7.3. For any prime p and $n \in \mathbb{N}$, $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\phi\rangle \cong \mathbb{Z}_n$, where ϕ is the Frobenius automorphism. So, the diagram of subfields of $\mathbb{F}_{p^n}$ is the same as the diagram of subgroups of the cyclic group $\mathbb{Z}_n$: for every $d \,\big|\, n$, the subfield $\mathbb{F}_{p^d}$ corresponds to the subgroup $\langle d\rangle$ of $\mathbb{Z}_n$: $\alpha \in \mathbb{F}_{p^d}$ iff $\varphi^d(\alpha) = \alpha^{p^d} = \alpha$. The subgroup $\langle d\rangle$ is isomorphic to $\mathbb{Z}_{n/d}$, and $\mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p) \cong \mathbb{Z}_n/\mathbb{Z}_{n/d} \cong \mathbb{Z}_d$.

4.7.4. Let $K \subset \mathbb{C}$ be the splitting field of $x^8 - 2 \in \mathbb{Q}[x]$ and $G = \mathrm{Gal}(K/\mathbb{Q})$. As we know from 4.5.6, $K = \mathbb{Q}(\alpha,\omega) = \mathbb{Q}(\alpha, i)$, where $\alpha = \sqrt[8]{2}$ and $\omega = \frac{1+i}{\sqrt{2}}$, G is generated by $\varphi : \alpha \mapsto \omega\alpha$, $i \mapsto i$, and $\psi : \alpha \mapsto \alpha$, $i \mapsto -i$, and has the presentation $G = \langle \varphi, \psi : \varphi^8 = \psi^2 = 1,\ \psi\varphi\psi^{-1} = \varphi^3\rangle$. (So, $G \cong \mathbb{Z}_8 \rtimes \mathbb{Z}_2 \cong SD_{16}$.) Let's find all normal subgroups of $G = \{1, \varphi, \ldots, \varphi^7, \psi, \varphi\psi, \ldots, \varphi^7\psi\}$. These are, of course, 1 and G itself. Next, these are $\langle\varphi\rangle$ and its cyclic subgroups $\langle\varphi^2\rangle$ and $\langle\varphi^4\rangle$. The identity $\varphi^{-1}\psi\varphi = \varphi^2\psi$ implies that the elements $\varphi^k\psi$ split into two conguacy classes, $\{\psi, \varphi^2\psi, \varphi^4\psi, \varphi^6\psi\}$ and $\{\varphi\psi, \varphi^3\psi, \varphi^5\psi, \varphi^7\psi\}$. If a normal subgroup N contains an element from one of these classes, then it contains all other elements of this class, so contains φ^2. If N also contains an element φ^k with an odd k, or contains an element of the other class, then it contains φ and coincides with G. Hence, we may only have, and do have, two more normal subgroups in G: $\langle\varphi^2, \psi\rangle$

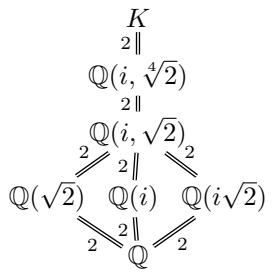
and $\langle\varphi^2, \varphi\psi\rangle$. Thus, the complete diagram of *normal* subgroups of G is



By duality, we must have an isomorphic diagram of normal subextensions of $K/\mathbb{Q}$:



Let's find the fields L_i:
(i) Since i is fixed by φ, we have $L_1 = \mathbb{Q}(i)$. (We need just one element of degree 2 to generate L_1.)
(ii) Both φ^2 and ψ fix $\sqrt{2}$, so $L_2 = \mathbb{Q}(\sqrt{2})$.
(iii) Both φ^2 and $\varphi\psi$ fix $i\sqrt{2}$, so $L_3 = \mathbb{Q}(i\sqrt{2})$.
(iv) φ^2 fixes i and $\sqrt{2}$, so $L_4 = \mathbb{Q}(i, \sqrt{2})$. (Indeed, L_4 is fixed by φ^2 and has degree 4 over $\mathbb{Q}$.)
(v) φ^4 fixes i and $\sqrt[4]{2}$ (since $\varphi^4(\alpha) = \alpha\omega^4 = -\alpha$), so $L_5 = \mathbb{Q}(i, \sqrt[4]{2})$.
So, the diagram of all normal subextensions of $K/\mathbb{Q}$ is



Let's find the Galois groups of K over the fields L_i. The groups $\mathrm{Gal}\big(K/\mathbb{Q}(i, \sqrt[4]{2})\big)$ and $\mathrm{Gal}\big(K/\mathbb{Q}(\sqrt{2}, i)\big)$ are generated by φ^4 and φ^2, and are isomorphic to $\mathbb{Z}_2$ and to $\mathbb{Z}_4$ respectively.

The group $\mathrm{Gal}\big(K/\mathbb{Q}(i)\big)$ is generated by φ and is isomorphic to $\mathbb{Z}_8$.

The group $\mathrm{Gal}\big(K/\mathbb{Q}(\sqrt{2})\big)$ is $\big\langle \varphi^2, \psi \bigm| (\varphi^2)^4 = \psi^2 = 1,\ \psi\varphi^2\psi^{-1} = (\varphi^2)^{-1}\big\rangle$ and is isomorphic to D_8.

The group $\mathrm{Gal}\big(K/\mathbb{Q}(i\sqrt{2})\big)$ is $\langle\varphi^2, \varphi\psi\rangle$. Let's put $a = \varphi^2$ and $b = \varphi\psi$, then a and b satisfy $a^4 = 1$; $b^2 = \varphi\psi\varphi\psi = \varphi^4 = a^2$, and so $b^4 = 1$; $bab^{-1} = \varphi\psi\varphi^2\psi^{-1}\varphi^{-1} = \varphi^6 = a^3 = a^{-1}$. These relations define the group $Q_8 = \big\langle a, b \bigm| a^4 = b^4 = 1,\ a^2 = b^2,\ bab^{-1} = a^{-1}\big\rangle$.

---

5. Composites and towers of Galois extensions

This is a rather technical section, which results will be helpful below.

5.1. The change of the basic field of a Galois extension

5.1.1. Theorem. *Let K/F be a Galois extension and L be any subfield of an extension of K. Then KL/FL is also Galois, and* $\mathrm{Gal}(KL/FL)$ *is (isomorphic to) a subgroup of* $\mathrm{Gal}(K/F)$.

Proof. The generators of K over F also generate KL over FL, so KL/FL is finite. These generators are all separable over F, so over FL. All conjugates of these elements over F, and so, over FL, are in K, so KL/FL is normal.

Any element φ of $\mathrm{Gal}(KL/FL)$ fixes F and defines an embedding $\varphi|_K : K/F \longrightarrow KL/F$; since K/F is normal, $\varphi(K) = K$, so $\varphi|_K \in \mathrm{Gal}(K/F)$. We therefore have a homomorphism $\mathrm{Gal}(KL/FL) \longrightarrow \mathrm{Gal}(K/F)$, $\varphi \mapsto \varphi|_K$. If $\varphi|_K$ is trivial, then φ fixes K, and since φ fixes L too, φ fixes KL, that is, is identical. Hence, the homomorphism $\varphi \mapsto \varphi|_K$ is injective, and $\mathrm{Gal}(KL/FL)$ is isomorphic to a subgroup of $\mathrm{Gal}(K/F)$. ∎

5.2. The composite of two extensions of which one is Galois

5.2.1. Theorem. *Let a Galois extension K/F be a composite $K = L_1L_2$ of two subextensions L_1/F and L_2/F such that $L_1 \cap L_2 = F$ and L_1/F is normal. Then* $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(K/L_1) \rtimes \mathrm{Gal}(L_1/F)$, $\mathrm{Gal}(K/L_2) \cong \mathrm{Gal}(L_1/F)$, *and* $[K : F] = [L_1 : F] \cdot [L_2 : F]$.

Proof. Let $G = \mathrm{Gal}(K/F)$, and let $H_1, H_2 \leq G$ be the subgroups corresponding to L_1 and L_2, $H_1 = \mathrm{Gal}(K/L_1)$ and $H_2 = \mathrm{Gal}(K/L_2)$. Then H_1 is normal in G, $H_1H_2 = G$, and $H_1 \cap H_2 = 1$, so $G = H_1 \rtimes H_2$, and $\mathrm{Gal}(L_1/F) \cong G/H_1 \cong H_2$:

$$\begin{array}{ccc} H_1 \cap H_2 = 1 & & L_1L_2 = K \\ {\scriptstyle m}\diagup\!\!\diagup \quad \diagdown\!\!\diagdown{\scriptstyle n} & & {\scriptstyle m}\diagup\!\!\diagup \quad \diagdown\!\!\diagdown{\scriptstyle n} \\ H_1 \qquad H_2 & & L_1 \qquad L_2 \\ {\scriptstyle n}\diagdown\!\!\diagdown \quad \diagup\!\!\diagup{\scriptstyle m} & & {\scriptstyle n}\diagdown\!\!\diagdown \quad \diagup\!\!\diagup{\scriptstyle m} \\ H_1H_2 = G & & L_1 \cap L_2 = F. \end{array}$$

Let $n = [L_1 : F]$ and $m = [L_2 : F]$; then $n = |G : H_1| = |H_2| = [K : L_2]$, $m = |G : H_2| = |H_1| = [K : L_1]$, and $[K : F] = nm$. ∎

5.2.2. Example. Let K be the splitting field of an irreducible polynomial $x^n - a \in \mathbb{Q}[x]$ for some $n \in \mathbb{N}$. Then $K = \mathbb{Q}(\omega, \alpha)$ where ω is a primitive nth root of unity and $\alpha = \sqrt[n]{a}$. So, K is the composite, $K = L_1L_2$, of the fields $L_1 = \mathbb{Q}(\omega)$ and $L_2 = \mathbb{Q}(\alpha)$. The extension $L_2/\mathbb{Q}$ is not, generally speaking, normal, and has degree n. The cyclotomic extension $L_1/\mathbb{Q}$ is normal, of degree $\varphi(n)$, and we have $\mathrm{Gal}(L_1/\mathbb{Q}) \cong \mathbb{Z}_n^*$ and $\mathrm{Gal}(K/L_1) \cong \mathbb{Z}_n$. It need not be that the intersection $L_1 \cap L_2 = \mathbb{Q}$, but if it is (say, if $(n, \varphi(n)) = 1$), then $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_n \rtimes \mathbb{Z}_n^*$.

5.3. The composite of two Galois extensions

5.3.1. Theorem. *Let an extension K/F be a composite $K = L_1L_2$ of two Galois subextensions L_1/F and L_2/F with $L_1 \cap L_2 = F$. Then K/F is Galois, and we have* $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(K/L_1) \times \mathrm{Gal}(L_1/F)$, $\mathrm{Gal}(K/L_2) \cong \mathrm{Gal}(L_1/F)$, $\mathrm{Gal}(K/L_1) \cong \mathrm{Gal}(L_2/F)$, *and* $[K : F] = [L_1 : F] \cdot [L_2 : F]$*:*

$$\begin{array}{ccc} H_1 \cap H_2 = 1 & & L_1L_2 = K \\ {\scriptstyle m}\diagup\!\!\diagup \quad \diagdown\!\!\diagdown{\scriptstyle n} & & {\scriptstyle m}\diagup\!\!\diagup \quad \diagdown\!\!\diagdown{\scriptstyle n} \\ H_1 \qquad H_2 & & L_1 \qquad L_2 \\ {\scriptstyle n}\diagdown\!\!\diagdown \quad \diagup\!\!\diagup{\scriptstyle m} & & {\scriptstyle n}\diagdown\!\!\diagdown \quad \diagup\!\!\diagup{\scriptstyle m} \\ H_1H_2 = G & & L_1 \cap L_2 = F. \end{array}$$

5.3.2. Examples. (i) Let K be the splitting field of the polynomial $f(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$. Then $K = L_1L_2$ where $L_1 = \mathbb{Q}(\sqrt{2})$ and $L_2 = \mathbb{Q}(\sqrt{3})$ are normal extensions of $\mathbb{Q}$, and $L_1 \cap L_2 = \mathbb{Q}$. Hence, $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(L_1/\mathbb{Q}) \times \mathrm{Gal}(L_2/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(ii) Let K be the splitting field of the polynomial $f(x) = (x^2 - 2)(x^3 - 3) \in \mathbb{Q}[x]$. Then $K = L_1L_2$, where $L_1 = \mathbb{Q}(\sqrt{2})$ and L_2 is the splitting field of $x^3 - 3$, $L_2 = \mathbb{Q}\big(e^{2\pi i/3}, \sqrt[3]{3}\big) = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{3})$. Both L_1 and L_2 are normal extensions of $\mathbb{Q}$, and $L_1 \cap L_2 = \mathbb{Q}$, so $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(L_1/\mathbb{Q}) \times \mathrm{Gal}(L_2/\mathbb{Q}) \cong \mathbb{Z}_2 \times S_3$.

5.3.3. Now let an extension K/F be a composite of two Galois subextensions L_1/F and L_2/F with $L_1 \cap L_2 \neq F$. Then K/F is Galois; let $G = \mathrm{Gal}(K/F)$, $H_1 = \mathrm{Gal}(K/L_1)$ and $H_2 = \mathrm{Gal}(K/L_2)$. By Theorem 5.3.1 we have the diagrams

$$\begin{array}{ccc} H_1 \cap H_2 = 1 \\ {\scriptstyle m}/\!/ \quad \backslash\!\backslash{\scriptstyle n} \\ H_1 \qquad H_2 \\ {\scriptstyle n}\backslash\!\backslash \quad /\!/{\scriptstyle m} \\ H_1H_2 \\ \|{\scriptstyle d} \\ G \end{array} \qquad\qquad \begin{array}{ccc} L_1L_2 = K \\ {\scriptstyle m}/\!/ \quad \backslash\!\backslash{\scriptstyle n} \\ L_1 \qquad L_2 \\ {\scriptstyle n}\backslash\!\backslash \quad /\!/{\scriptstyle m} \\ L_1 \cap L_2 \\ \|{\scriptstyle d} \\ F \end{array}$$

where $H_1H_2 = H_1 \times H_2$, and $[K : F] = [L_1 : F] \cdot [L_2 : F]/[L_1 \cap L_2 : F]$.

Let $N_1 = \mathrm{Gal}(L_1/F)$ and $N_2 = \mathrm{Gal}(L_2/F)$. Then $N_1 \cong G/H_1$, and $H_1 \cong (H_1H_2)/H_2$ is isomorphic to a (normal) subgroup of $N_2 \cong G/H_2$, that is, G "is made of" N_1 and a subgroup of N_2.

5.3.4. Here is a more detailed description of the group G from 5.3.3. We have a natural homomorphism $\eta\colon G \longrightarrow N_1 \times N_2$, $\varphi \mapsto (\varphi|_{L_1}, \varphi|_{L_2})$, which is injective since $L_1L_2 = K$. η is not, however, surjective: if $\varphi_1 = \varphi|_{L_1}$ and $\varphi_2 = \varphi|_{L_2}$, then $\varphi_1|_{L_1\cap L_2} = \varphi_2|_{L_1\cap L_2}$. Let $D = \mathrm{Gal}\big((L_1 \cap L_2)/F\big)$, then $D = G/(H_1H_2) \cong N_1/\big((H_1H_2)/H_2\big) \cong N_2/\big((H_1H_2)/H_1\big)$ is a common factor of N_1 and N_2; let $\tau_1\colon N_1 \longrightarrow D$ and $\tau_1\colon N_2 \longrightarrow D$ be the factorization mappings. Then the image of η lies in the subgroup

$$N_1 \times_D N_2 = \big\{(\varphi_1, \varphi_2) : \tau_1(\varphi_1) = \tau_2(\varphi_2)\big\}$$

of $N_1 \times N_2$, called *the relative direct product* of the groups N_1 and N_2 with respect to their common factor D. Comparing their cardinalities, we find that $G \cong N_1 \times_D N_2$.

5.3.5. Example. Let K be the splitting field of the polynomial $f(x) = (x^3 - 2)(x^3 - 3) \in \mathbb{Q}[x]$. Then $K = L_1L_2$, where L_1 and L_2 are the splitting fields of $x^3 - 2$ and of $x^3 - 3$ respectively, $L_1 = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$ and $L_1 = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{3})$. Both L_1 and L_2 are normal extensions of $\mathbb{Q}$, $L_1 \cap L_2 = \mathbb{Q}(\sqrt{-3})$, so $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(L_1/\mathbb{Q}) \times_{\mathrm{Gal}((L_1\cap L_2)/\mathbb{Q})} \mathrm{Gal}(L_2/\mathbb{Q}) \cong S_3 \times_{\mathbb{Z}_2} S_3$.

5.4. Free composites of Galois extensions

5.4.1. Let us say that a composite $K = L_1 \cdots L_n$ of algebraic extensions L_i/F is *free* if the natural epimorphism $L_1 \otimes_F \cdots \otimes_F L_n \longrightarrow K$ is an isomorphism. If L_i/F are all finite, this is equivalent to having $[K : F] = \prod_{i=1}^n [L_i : F]$. In the case $K = L_1 \cdots L_n$ is a free composite, for each i we have $L_i \cap \big(L_1 \cdots L_{i-1}L_{i+1} \cdots L_n\big) = F$.

5.4.2. Let K/F be a Galois extension whose Galois group $G = \mathrm{Gal}(K/F)$ is a direct product, $G = H_1 \times \cdots \times H_k$, of subgroups $H_1, \ldots, H_n$. Then each of H_i is normal in G. For each i put $N_i = H_1 \times \cdots \times H_{i-1} \times H_{i+1} \times \cdots \times H_n$; then N_i are normal subgroups of G with $G/N_i \cong H_i$, and $N_1 \cap \cdots \cap N_n = 1$. For each $i = 1, \ldots, n$, let $L_i = \mathrm{Fix}(N_i)$; then L_i/F are Galois extensions with $\mathrm{Gal}(L_i/F) \cong G/N_i \cong H_i$. We have $L_1 \cdots L_n = K$ and $\prod_{i=1}^n [L_i : F] = \prod_{i=1}^n |H_i| = |G|$, so K is a free composite of $L_1, \ldots, L_n$.

5.4.3. Conversely, if an extension K/F is a composite, $K = L_1 \cdots L_n$, of Galois subextensions L_i/F with $\mathrm{Gal}(L_i/F) = H_i$, $i = 1, \ldots, n$, such that for each i, $L_i \cap \big(L_1 \cdots L_{i-1}L_{i+1} \cdots L_n\big) = F$, then by 5.3.1, K/F is Galois with $\mathrm{Gal}(K/F) \cong H_1 \times \cdots \times H_n$, and is a free composite of $L_1/F, \ldots, L_n/F$.

5.5. Composites of towers of Galois extensions

5.5.1. Let K/F be a Galois extension, and assume that K is a tower,

$$K = L_n/L_{n-1}/\cdots/L_1/L_0 = F, \tag{5.1}$$

of Galois extensions, that is, with L_i/L_{i-1} being Galois for all i. For each i, let $H_i = \mathrm{Gal}(K/L_i)$; then G has the subnormal series

$$1 = H_n \trianglelefteq H_{n-1} \trianglelefteq \cdots \trianglelefteq H_1 \trianglelefteq H_0 = G, \tag{5.2}$$

where for each i, $H_{i-1}/H_i \cong \mathrm{Gal}(L_i/L_{i-1})$.

Conversely, if K/F is a Galois extension whose Galois group G possesses a subnormal series (5.2), then K/F is representable as a tower of Galois extensions (5.1), where for each i, $L_i = \mathrm{Fix}(H_i)$, and $\mathrm{Gal}(L_i/L_{i-1}) \cong H_{i-1}/H_i$.

5.5.2. Let $K = L_n/L_{n-1}/\cdots/L_1/L_0 = F$ and $K' = L'_m/L'_{m-1}/\cdots/L'_1/L'_0 = F$ be two towers of Galois extensions, contained in a common field. Then the composite KK' is representable as the tower

$$KK' = (L_nL'_m)/(L_nL'_{m-1})/\cdots/(L_nL'_1)/L_n/L_{n-1}/\cdots/L_1/L_0 = F.$$

of Galois extensions, and by Theorem 5.1.1 or by 5.1.1, for each j the group $\mathrm{Gal}\big((L_nL'_j)/(L_nL'_{j-1})\big)$ is isomorphic to a subgroup of $\mathrm{Gal}(L'_j/L'_{j-1})$. We obtain:

Theorem. *The composite of two towers of Galois extensions, with Galois groups $N_1, \dots, N_r$, is a tower of Galois extensions, whose Galois groups are subgroups of $N_1, \dots, N_r$.*

5.5.3. If K/L and L/F are Galois extensions, the extension K/F may not be Galois. By Theorem 4.4.3, K/F is separable; let E/F be the Galois closure of K/F, let $\mathrm{Gal}(E/F) = \{\varphi_1, \dots, \varphi_n\}$. E is generated by the conjugates of K, so E is the composite $E = K_1 \cdots K_n$ where for each i, $K_i = \varphi_i(K)$. Since the extension L/F is normal, for each i, $\varphi_i(L) = L$, so K_i is an extension of L, and we have the commutative diagram

$$\begin{array}{ccc} \varphi_i{:}K & \xrightarrow{\sim} & K_i \\ \| & & \| \\ L & \xrightarrow{\sim} & L. \\ & \searrow \quad \swarrow & \\ & F & \end{array}$$

(We cannot say, however, that K_i/L is isomorphic to K/L since φ_i does not, generally speaking, fix L.) Since φ is an isomorphism, $\mathrm{Gal}(K_i/L) \cong \mathrm{Gal}(K/L)$.

5.5.4. Example. Let $\alpha = \sqrt[4]{2}$, so that $\alpha^2 = \sqrt{2}$. Let $K = K_1 = \mathbb{Q}(\alpha)$ and $L = \mathbb{Q}(\alpha^2)$. The extensions K/L and $L/\mathbb{Q}$ are quadratic and so Galois, but the extension $K/\mathbb{Q}$ is not. The conjugates of α over $\mathbb{Q}$ are $\pm\alpha$, $\pm i\alpha$ (where $i = \sqrt{-1}$), and the Galois closure of $K/\mathbb{Q}$ is $\mathbb{Q}(\alpha, i\alpha) = K_1K_2$ where $K_2 = \mathbb{Q}(i\alpha)$. The field K_2 is also a quadratic extension of L, the minimal polynomial of its generator $i\alpha$ over L is $x^2 + \alpha^2$. The homomorphism φ that produces the commutative diagram

$$\begin{array}{ccc} \varphi{:}K & \xrightarrow{\sim} & K_2 \\ \| & & \| \\ L & \xrightarrow{\sim} & L \\ & \searrow \quad \swarrow & \\ & \mathbb{Q} & \end{array}$$

is defined by $\varphi(\alpha) = i\alpha$, and maps α^2 to $-\alpha^2$.

5.5.5. Let $K = L_n/L_{n-1}/\cdots/L_1/L_0 = F$ be a tower of Galois extensions. By Theorem 4.4.3, K/F is separable; let E/F be the Galois closure of K/F, and let $G = \mathrm{Gal}(E/F)$. Then E/F is the composite of the extensions $\varphi(K)/F$, $\varphi \in G$, and for each φ, this extension is the tower $\varphi(K) = \varphi(L_n)/\varphi(L_{n-1})/\cdots/\varphi(L_1)/\varphi(L_0) = F$ of Galois extensions with $\mathrm{Gal}\big(\varphi(L_i)/\varphi(L_{i-1})\big) \cong \mathrm{Gal}(L_i/L_{i-1})$ for all i. By Theorem 5.5.2, we obtain:

Theorem. *If K/F is a tower of Galois extensions, with Galois groups $N_1, \dots, N_r$, then the Galois closure E/F of K/F is also a tower of Galois extensions, whose Galois groups are subgroups of $N_1, \dots, N_r$. It follows that* $\mathrm{Gal}(E/F)$ *has a subnormal series with factors being subgroups of $N_1, \dots, N_r$.*

---

6. Some applications of the Galois theory

6.1. More methods of finding the minimal polynomial

6.1.1. Let α be a separable algebraic element over a field F. Construct a Galois extension K/F that contains α and find $G = \mathrm{Gal}(K/F)$. Find the orbit $G\alpha = \{\alpha_1, \dots, \alpha_n\}$ of α under the action of G; then $\alpha_1, \dots, \alpha_n$ are all the conjugates of α over F, and the minimal polynomial of α is $m_{\alpha,F}(x) = \prod_{i=1}^{n}(x - \alpha_i)$.

We also have that $\prod_{\varphi \in \mathrm{Gal}(K/F)}(x - \varphi(\alpha)) = m_{\alpha,F}^k$ for some k. Comparing the degrees, we see that $\deg m_{\alpha,F} = [F(\alpha) : F]$ and $\deg \prod_{\varphi \in \mathrm{Gal}(K/F)}(x - \varphi(\alpha)) = [K : F]$, so $k = [K : F]/[F(\alpha) : F] = [K : F(\alpha)]$.

Example. Let's find the minimal polynomial of $\alpha = \sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$. We have $\alpha \in K = \mathbb{Q}\big(\sqrt{2},\sqrt{3}\big)$, whose the Galois group $G = \mathrm{Gal}(K/\mathbb{Q}) \cong V_4$ acts by $\sqrt{2} \mapsto \pm\sqrt{2}$ and $\sqrt{3} \mapsto \pm\sqrt{3}$. The set of conjugates of α is the orbit of α under the action of G, which is

$$\Big\{\alpha_1 = \sqrt{2}+\sqrt{3},\ \alpha_2 = -\sqrt{2}+\sqrt{3},\ \alpha_3 = \sqrt{2}-\sqrt{3},\ \alpha_4 = -\sqrt{2}-\sqrt{3}\Big\}.$$

The minimal polynomial of α is therefore

$$f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4) = \big(x^2-(5+2\sqrt{6})\big)\big(x^2-(5-2\sqrt{6})\big) = x^4-10x^2+25-24 = x^4-10x^2+1.$$

And without any computations, since the orbit of α has 4 elements, $\deg_{\mathbb{Q}} \alpha = 4$.

6.1.2. Let α be a separable algebraic element over a field F, let K/F be a Galois extension that contains α, let L/F be a normal subextension of K/F, and let $p = m_{\alpha,L}$, the minimal polynomial of α over L. The minimal polynomial $m_{\alpha,F}$ of α over F splits over L to a product or irreducible polynomials, the minimal polynomials of their roots; for every $\varphi \in \mathrm{Gal}(K/F)$, $\varphi(p)$ is contained and is irreducible in $L[x]$, and its roots are conjugate of α; thus, these are the other irreducible factors of $m_{\alpha,F}$ over L. (In particular, all these factors have the same degree.) Since L/F is normal, $\varphi \in \mathrm{Gal}(K/F)$ induce elements of $\mathrm{Gal}(L/F)$; so, $m_{\alpha,F}$ is the product of distinct polynomials $\varphi(p)$, $\varphi \in \mathrm{Gal}(L/F)$.

We also have that $\prod_{\varphi\in\mathrm{Gal}(L/F)} \varphi(p) = m_{\alpha,F}^k$ for some k. Comparing the degrees, we see that $\deg m_{\alpha,F} = [F(\alpha):F]$ and $\deg \prod_{\varphi\in\mathrm{Gal}(L/F)} \varphi(p) = [L:F]\cdot[L(\alpha):L]$, so $k = [L:F]\cdot[L(\alpha):L]/[F(\alpha):F] = [L(\alpha):F(\alpha)]$.

Example. Again, let $F = \mathbb{Q}$ and $\alpha = \sqrt{2}+\sqrt{3}$. Take $L = \mathbb{Q}(\sqrt{2})$. Then $p(x) = m_{\alpha,L}(x) = (x-\sqrt{2})^2 - 3 = x^2 - 2\sqrt{2}x - 1$. We have $L(\alpha) = \mathbb{Q}(\alpha)$, so $m_{\alpha,\mathbb{Q}} = p\varphi(p)$ where $\varphi : \sqrt{2} \mapsto -\sqrt{2}$, so $m_{\alpha,\mathbb{Q}} = (x^2 - 2\sqrt{2}x - 1)\cdot(x^2 + 2\sqrt{2}x - 1) = x^4 - 2x^2 + 1 - 8x^2 = x^4 - 10x^2 + 1$.

6.2. The norm of algebraic elements

6.2.1. Let K/F be a Galois extension, let $G = \mathrm{Gal}(K/F)$. For every $\alpha \in K$ define *the norm* of α (in K and over F) by the formula $N_{K/F}(\alpha) = \prod_{\varphi\in G} \varphi(\alpha)$. In the case $\deg_F \alpha = [K:F]$, that is, when $K = F(\alpha)$, all elements $\varphi(\alpha)$, $\varphi \in G$, are distinct, and $N_{K/F}(\alpha)$ is the product of all the conjugates of α; otherwise, it is the product of all conjugates of α to the power of $[K : F(\alpha)]$.

For any α, since $N_{K/F}(\alpha)$ is fixed by G, we have $N_{K/F}(\alpha) \in F$. From the very definition, $N_{K/F}$ is multiplicative: $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$. Hence, $N_{K/F}$ is a homomorphism of the multiplicative groups $K^* \longrightarrow F^*$ (and $N_{K/F}(0) = 0$).

6.2.2. Example. If K/F is a quadratic extension, $K = F(\sqrt{D})$, then for $\alpha = a + b\sqrt{D} \in K$, $a, b \in F$, we have $N_{K/F}(\alpha) = (a+b\sqrt{D})(a-b\sqrt{D}) = a^2 - b^2D$. This is just the norm that was so helpful to us in the first semester when we dealt with the rings of quadratic integers.

6.2.3. Now let K/F be a finite separable extension, let $[K:F] = n$. Let E/F be any Galois extension containing K, let $G = \mathrm{Gal}(E/F)$ and $H = \mathrm{Gal}(E/K)$. For $\alpha \in K$, define *the norm* of α in K over F by $N_{K/F}(\alpha) = \prod_{\varphi\in G/H} \varphi(\alpha)$. (Where G/H is the set of left cosets of H in G; it is not a group if H is not normal in G.) Notice that for φ, ψ from the same left coset of H in G, $\varphi(\alpha) = \psi(\alpha)$, so the formula above defines $N_{K/F}(\alpha)$ well.

In the case $E = K$, this coincides with the definition in 6.2.1.

6.2.4. We have the following:

Proposition. (i) *$N_{K/F}$ does not depend on the choice of the extension E.*

(ii) *$N_{K/F}(\alpha) \in F$ for all $\alpha \in K$.*

(iii) *$N_{K/F}$ is a multiplicative function from K to F, $N_{K/F}(\alpha_1\alpha_2) = N_{K/F}(\alpha_1)N_{K/F}(\alpha_2)$ for any $\alpha_1, \alpha_2 \in K$.*

(iv) *For $\alpha \in K$, let $m_{\alpha,F}(x) = x^d + \cdots + a_1x + a_0$; then $N_{K/F}(\alpha) = (-1)^n a_0^{n/d}$.*

(v) *For $\alpha \in K$, let T be the linear transformation of K defined by multiplication by α, $T(\beta) = \alpha\beta$. Then $N_{K/F}(\alpha) = \det T$.*

Proof. (ii) follows from the fact that for every $\alpha \in K$, $N_{K/F}(\alpha)$ is fixed by G.

(iii) is clear from the definition.

The product of all conjugates of α is $(-1)^d a_0$, where $d = \deg_F \alpha$. In the product $\prod_{\varphi\in G} \varphi(\alpha)$ each conjugate of α appears $|G|/d$ times, and in the product $N_{K/F}(\alpha) = \prod_{\varphi\in G/H} \varphi(\alpha)$ it appears $(|G|/|H|)/d = n/d$ times. So, $N_{K/F}(\alpha) = (-1)^n a_0^{n/d}$, which proves (iv).

(i) follows from (iv).

Finally, in (v), the characteristic polynomial of T is $c_T = m_{\alpha,F}^{n/d}$. Hence, $\det T$, which is the constant term of c_T times $(-1)^n$, equals $N_{K/F}(\alpha)$ by (iv). ■

6.3. Abelian extensions

Let K/F be an abelian extension, that is, a Galois extension whose Galois group G is abelian.

6.3.1. Every subgroup of G is normal, so every subextension of K/F is normal. This implies that for every $\alpha \in K$, $F(\alpha)$ contains all conjugates of α.

6.3.2. By the fundamental theory of abelian groups, G is a direct product of cyclic subgroups, $G = H_1 \times \cdots \times H_k$, $H_i \cong \mathbb{Z}_{n_i}$ for some $n_i \in \mathbb{N}$, $i = 1, \ldots, k$. By 5.4, K is a free composite of cyclic subextensions: $K = L_1 \cdots L_n$ where for every i, $L_i = \mathrm{Fix}\big(H_1 \times \cdots \times H_{i-1} \times H_{i+1} \times \cdots \times H_k\big)$, L_i/F are Galois with $\mathrm{Gal}(L_i/F) \cong H_i$, and $L_i \cap \big(L_1 \cdots L_{i-1}L_{i+1} \cdots L_k\big) = F$, $i = 1, \ldots, k$.

6.3.3. Any cyclotomic extension is abelian, so is a free composite of cyclic subextensions.

6.4. Subextensions of the real radical extension $F(\sqrt[n]{a})/F$, $a > 0$, and the Galois group of $x^n - a$

Let F be a real field (that is, $F \subseteq \mathbb{R}$), let $a \in F$, $a > 0$, let $n \in \mathbb{N}$, and assume that the polynomial $x^n - a$ is irreducible in $F[x]$.

6.4.1. Claim. *The only subextensions of $F(\sqrt[n]{a})/F$ are subextensions of the form $F(\sqrt[d]{a})/F$ with $d \,\big|\, n$. In particular, the only nontrivial normal subextension of $F(\sqrt[n]{a})/F$, and only if n is even, is $F(\sqrt{a})/F$.*

Proof. Let $\alpha = \sqrt[n]{a} \in \mathbb{R}$ and $K = F(\alpha)$. Let L/F be a subextension of K/F, with $[L : F] = d$; then $\deg_L \alpha = n/d$. Let β be the product of the conjugates of α over L, then $\beta \in L$, All conjugates of α over F have form $\omega^k\alpha$, where $\omega = e^{2\pi i/n}$; so, $\beta = \alpha^{n/d}\omega^r$ for some r. But since $\beta \in \mathbb{R}$, $\omega^r = \pm 1$, so $\beta = \pm\alpha^{n/d} = \pm\sqrt[d]{a}$. Since $\deg_F \sqrt[d]{a} = d = [L : F]$, we obtain that $L = F(\sqrt[d]{a})$. (The polynomial $x^d - a$ is irreducible in $F[x]$ since otherwise $x^n - a = (x^{n/d})^d - a$ would also be reducible.)

If $d \geq 3$, then $F(\sqrt[d]{a})/F$ is not normal, since $\sqrt[d]{a}$ has nonreal conjugates. ■

6.4.2. Let $\alpha = \sqrt[n]{a} \in \mathbb{R}$, $\omega = e^{2\pi i/n}$, $K = F(\alpha)$, and $N = F(\omega)$; then $KN = F(\omega, \alpha)$ is the splitting field of $x^n - a$. Since N/F is abelian, the extension $(K \cap N)/F$ is a normal subextension of K/F, so either $K \cap N = F$, or, if n is even and $\sqrt{a} \in N$, is a quadratic extension.

If $F = \mathbb{Q}$, in the first case we have $[KN : F] = n\varphi(n)$ and $\mathrm{Gal}(x^n - a) = \mathrm{Gal}(KN/\mathbb{Q}) \cong \mathbb{Z}_n \rtimes \mathbb{Z}_n^*$, and in the second case $[KN : \mathbb{Q}] = n\varphi(n)/2$.

6.4.3. Examples. (i) The splitting field of $f = x^8 - 3 \in \mathbb{Q}[x]$ is KN where $K = \mathbb{Q}\big(\sqrt[8]{3}\big)$ and $N = \mathbb{Q}\big(\frac{1+i}{\sqrt{2}}\big)$. It is easy to see that $K \cap N = \mathbb{Q}$, so $\mathrm{Gal}(f/\mathbb{Q}) \cong \mathbb{Z}_8 \rtimes \mathbb{Z}_8^*$, $|G| = 32$.

(ii) The splitting field of $f = x^8 - 2 \in \mathbb{Q}[x]$ is KN where $K = \mathbb{Q}\big(\sqrt[8]{2}\big)$ and $N = \mathbb{Q}\big(\frac{1+i}{\sqrt{2}}\big)$. This time $K \cap N = \mathbb{Q}(\sqrt{2})$, and $|G| = 16$. (G is the semidihedral group SD_{16}.)

6.5. The theorem on a primitive element

6.5.1. We will need the following nice fact:

Proposition. *Any finite separable extension has only finitely many subextensions.*

Proof. Any such extension is contained in a Galois extension (the Galois closure thereof), which has only finitely many subextensions (corresponding to (finitely many) subgroups of its Galois group). ■

6.5.2. An element α of an algebraic extension K/F is said to be *primitive* if $K = F(\alpha)$.

6.5.3. Theorem. *Every finite separable extension is simple (that is, possesses a primitive element).*

Proof. Let K/F be a finite separable extension. Consider two cases.

(i) F is finite. In this case K is also a finite field, and is a simple extension of $\mathbb{F}_p$.

(ii) F is infinite. Then the union of any finite collection of proper subspaces of K viewed as an F-vector space is a proper subset of K. Since K has only finitely many proper subfields that are subextensions of K/F, there is an element $\alpha \in K$ that is not contained in any of these subfields (see Lemma below). Hence, $F(\alpha) = K$. ■

Lemma. *If F is an infinite field and V is an F-vector space, then V is not a union of its proper subspaces.*

Proof. Assume that $V = \bigcup_{i=1}^{n} V_i$ for $n \geq 2$. We may assume that $V_1 \not\subseteq \bigcup_{i=2}^{n} V_i$, otherwise we can exclude V_1. Let $\alpha \in V_1 \setminus \bigcup_{i=2}^{n} V_i$ and $\beta \notin V_1$, and consider the line $L = \{\alpha t + \beta(1-t),\ t \in F\}$. We have $L \cap V_1 = \{\alpha\}$; L is infinite, so there is $i \geq 2$ and distinct $t_1, t_2 \in F$ such that $\alpha t_1 + \beta(1-t_1), \alpha t_2 + \beta(1-t_2) \in V_i$. But then $\alpha \in V_i$, contradiction. ■

6.5.4. Corollary. *Let L/F be a finite separable extension of degree n, and let K/F be the Galois closure of L/F. Then* $\mathrm{Gal}(K/F)$ *is (isomorphic to) a subgroup of S_n.*

Proof. Let α be a primitive element of L with respect to F. Then every conjugate of L in K is generated by a conjugate of α, and K is generated by the set A of conjugates of α. Any automorphism of K/F is defined by its actions on A. Since $|A| = \deg_F \alpha = [L : F] = n$, $\mathrm{Gal}(K/F)$ is isomorphic to a subgroup of S_n. ■

6.5.5. Theorem 6.5.3 does not hold for inseparable extensions: take $K = \mathbb{F}_p(x, y)$ (the field of rational functions in two variables over $\mathbb{F}_p$) and $F = \mathbb{F}_p(x^p, y^p)$; then $[K : F] = p^2$, but for every element $h \in K$, $h^p \in F$, so $[F(h) : F] \leq p$. (Indeed, for any $f \in \mathbb{F}_p[x, y]$, $f(x, y)^p = f(x^p, y^p) \in F$ and for any $f/g \in K$, $(f/g)^p = f^p/g^p \in F$ too.)

6.6. p-extensions

Let p be a prime integer.

6.6.1. A Galois extension K/F is said to be *a p-extension* if $[K : F] = p^n$ for some $n \in \mathbb{N}$ (and so, $\mathrm{Gal}(K/F)$ is a p-group).

A finite extension is *a p-extension* if it is contained in a Galois p-extension. For Galois extensions these two definitions coincide: if K/F is Galois and is a subextension of a Galois p-extensions E/F, then $\mathrm{Gal}(K/F)$ is a quotient group of $\mathrm{Gal}(E/F)$ and so, is a p-group.

6.6.2. The degree of any p-extension is a power of p. The converse is not true: the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ has degree 3 but is not a 3-extension.

6.6.3. Theorem. *An extension is a p-extension iff it is a tower of cyclic Galois extensions of degree p.*

Proof. Let K/F be a p-extension, let $K \subseteq E$ such that E/F is Galois with $G = \mathrm{Gal}(E/F)$ being a p-group. Let $H = \mathrm{Gal}(E/K)$, then $H \leq G$, $|H| = p^k$ for some k. By Sylow's theory, or by the theory of p-groups, there is a series $H = H_k \leq H_{k+1} \cdots \leq H_n = G$ of subgroups of G such that $|H_i| = p^i$ for each i. Since, for each i, $|H_i : H_{i-1}| = p$, H_{i-1} is a normal subgroup of H_i, with $H_i/H_{i-1} \cong \mathbb{Z}_p$. For each i, let $L_i = \mathrm{Fix}(H_i)$, then we have a tower $K = L_k/L_{k+1}/\cdots/L_n = F$ such that for every i, L_{i-1}/L_i is Galois with $\mathrm{Gal}(L_{i-1}/L_i) \cong \mathbb{Z}_p$.

Conversely, let $K = L_0/L_1/\cdots/L_n = F$, where for every i, L_{i-1}/L_i is Galois with the Galois group $\cong \mathbb{Z}_p$. Then K/F is seprable; let E be the Galois closure of K; then E is a composite of towers isomorphic to the tower of K, so is itself a tower of Galois extensions with Galois groups isomorphic to a subgroup of $\mathbb{Z}_p$ (which is either $\mathbb{Z}_p$ or is trivial), so $[E : F] = p^n$. ■

We also see from the proof that a finite extension is a p-extension iff it is separable and its Galois closure is a p-extension.

6.6.4. Theorem. (i) *If K/F is a p-extension and L/F is a subextension of K/F, then both K/L and L/F are p-extension.*

(ii) *If L_1/F and L_2/F are p-subextensions of an extension K/F, then their composite L_1L_2/F is a p-extension.*

(iii) *If K/L and L/F are p-extensions, then K/F is also a p-extension.*

6.6.5. Since any separable quadratic extension is Galois, an extension is a 2-extension iff it is a tower of separable quadratic extensions; we will say that it is *polyquadratic* in this case.

6.7. The fundamental theorem of algebra

6.7.1. The fundamental theorem of algebra can be proved with the help of the Galois theory:

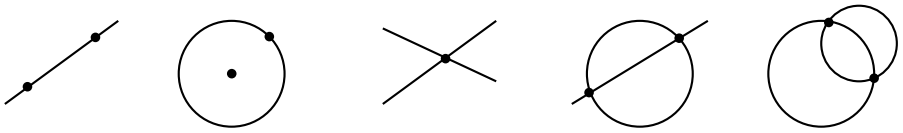
Theorem. *$\mathbb{C}$ is the algebraic closure of $\mathbb{R}$ (and so, is algebraically closed).*

Proof. The proof is based on two facts:
(i) Any polynomial over $\mathbb{R}$ of odd degree has a root in $\mathbb{R}$ and so, is either linear or reducible in $\mathbb{R}[x]$.
(ii) For any $a \in \mathbb{R}$, $\sqrt{a} \in \mathbb{R}$ if $a > 0$ and $\mathbb{R}(\sqrt{a}) \cong \mathbb{C}$ if $a < 0$. For any $z \in \mathbb{C}$, $\sqrt{z} \in \mathbb{C}$ (for $z = a + bi$, $w = \frac{1}{\sqrt{2}}\sqrt{\sqrt{a^2+b^2}+a} + \frac{i\,\mathrm{sign}(b)}{\sqrt{2}}\sqrt{\sqrt{a^2+b^2}-a}$, where all radicals are ≥ 0). Since every (separable) quadratic extension is obtained by adjoining a square root, this implies that $\mathbb{C}$ is the only (up to isomorphism) quadratic extension of $\mathbb{R}$ and has no quadratic extensions itself.

I'll show that every nontrivial finite extension L of $\mathbb{R}$ is isomorphic to $\mathbb{C}$. Let $K/\mathbb{R}$ be the Galois closure of $L/\mathbb{R}$, let $G = \mathrm{Gal}(K/\mathbb{R})$. Let H be the Sylow 2-subgroup of G and let $N = \mathrm{Fix}(H)$. Then for every $\alpha \in N$, the polynomial $m_{\alpha,\mathbb{R}}$ has odd degree, which is, by (i), impossible unless $\alpha \in \mathbb{R}$. Hence, $N = \mathbb{R}$ and $H = G$. Then G is a 2-group, $K/\mathbb{R}$ is a 2-extension and is a tower $K = L_0/L_1/\cdots/L_k = \mathbb{R}$ of quadratic extensions. By (ii) we see that either $K = \mathbb{R}$ or $K/\mathbb{R} \cong \mathbb{C}/\mathbb{R}$ (and so, $L = \mathbb{R}$ or $L/\mathbb{R} \cong \mathbb{C}/\mathbb{R}$). ■

6.8. Constructions with ruler and compass

6.8.1. Given a set S of points on the Euclidean plane, of cardinality ≥ 2, the following *constructions with ruler and compass* are allowed to produce new points and add them to S: (i) connecting two of the points by a straight line; (ii) drawing a circle centered at one of the points and passing through another; (iii) finding (and adding to S) the points of intersection of two lines, of a line and a circle, or of two circles already constructed. The points constructible this way are said to be *constructible* (from S, with ruler and compass).



6.8.2. Let S be a set of (more than one) points on the plane. Let us introduce a Cartesian coordinate system on the plane (using points of S as the origin and a unit coordinate vector). A real number is said to be *constructible* (from S) if it represents a coordinate of a constructible (from S) point. Clearly, a point on the plane is constructible (from S) iff both its coordinates are constructible (from S) numbers.

6.8.3. It is easy to see that the coordinates of the numbers constructible from a set S form a field: if we have points whose (first or second) coordinates are a and b, then we can construct points whose (say, first) coordinates are $a+b$, $a-b$, ab, or a/b. Moreover, we can also construct a point with coordinate $\sqrt{a}$, so this field is closed under taking quadratic extensions ("is quadratically closed").

Let F be the field generated by the coordinates of the points of S. If a real number a is constructible from S, we will also say that a is *constructible over F*. A real number is said to be just *constructible* if it is constructible over $\mathbb{Q}$.

6.8.4. Let S be a set of points in the plane and F be the field generated by the coordinates of the points from S. The coordinates of any new point obtained from the points of S by the operations (i)-(iii) are solutions of either a linear or a quadratic equation with coefficients from the field, generated by the coordinates of S, and so, either belong to F or to a quadratic extension of F. Hence, we have:

Proposition. *A real number is constructible over a real (that is, contained in $\mathbb{R}$) field F iff it is contained in a real polyquadratic extension of F.*

6.8.5. The restriction that the constructible numbers must be real is inconvenient, and we can get rid of it. A complex number $\gamma = \alpha + \beta i$, $\alpha, \beta \in \mathbb{R}$, is said to be *constructible* over a real field F iff both α and β are constructible over F. (Thus, if we interprete the plane as the complex plane, a complex number is constructible iff the correponding point is constructible.) Then we also have:

Proposition. *A complex number is constructible over a real field F iff it is contained in a polyquadratic extension of F.*

Proof. If a complex number $\gamma = \alpha + \beta i$ is constructible, that is, both α and β are contained in towers of real quadratic extensions, then the composite of these towers is also a real polyquadratic tower, which contains both α and β, and γ is contained in the (quadratic) extension of this tower obtained by adjoining i.

Conversely, assume that $\gamma = \alpha + \beta i$ is contained in a tower $K = L_n/L_{n-1}/\dots/L_0 = F(i)$ of quadratic extensions of $F(i)$. For every j let L'_j be the complex conjugate of L_j, let $M_j = L_j L'_j$, and let $N_j = M_j \cap \mathbb{R}$. Then we have the tower $N = N_n/N_{n-1}/\dots/N_0 = F$ of real extensions, and $\alpha, \beta \in N$. I claim that for every j, the extension N_j/N_{j-1} is a tower of at most two quadratic extensions. Indeed, let $L_j = L_{j-1}(z)$ where $z = x + yi = \sqrt{c}$ for some $c = a + bi \in L_{j-1}$, then $L'_j = L'_{j-1}(\bar{z})$ and $M_j = M_{j-1}(z, \bar{z}) = M_{j-1}(x, y)$. So $N_j = N_{j-1}(x, y)$. (There is a basis in M_j over M_{j-1} consisting of elements of the form $x^r y^s$ for some r, s, and a linear combination of such elements is in N_j iff all the coefficients are real, that is, are from N_{j-1}.) But $x^2 - y^2 = a$ and $2xy = b$, so $x = \sqrt{\big(\sqrt{a^2 + b^2} + a\big)/2}$ and $y = b/2x$, with $a, b \in N_{j-1}$. ∎

6.8.6. From 6.6.5 we obtain:

Theorem. *A complex number α is constructible over a real field F iff the splitting field of $m_{\alpha,F}$ is a 2-extension.*

6.8.7. As a corollary we see that the following problems are non-solvable with ruler and compass:

(i) *Squaring a circle*: Construct a square that has the same area as the unit circle; in other words, construct $a \in \mathbb{R}$ such that $a^2 = \pi$.

Indeed, the number $\sqrt{\pi}$ is transcendental.

(ii) *Doubling the cube*: Construct a cube having the volume of two unit cubes; or, in coordinates: find an $a \in \mathbb{R}$ such that $a^3 = 2$.

Indeed, $\sqrt[3]{2}$ is not contained in any 2-extension.

(iii) *Trisecting an angle*: Given an angle θ, construct the angle $\theta/3$. This problem is equivalent to the problem of constructing the cubic root of a complex number of absolute value 1. It is solvable for some θ (for $\theta = \pi$ for instance), but non-solvable in general. (For example, the angle of $\pi/3$ is not trisectable, as we will see right below.)

6.8.8. Consider the problem of constructing (over $\mathbb{Q}$) of a regular n-gon. This problem is equivalent to constructing the complex number $\omega = e^{2\pi i/n}$, that is, a primitive root of unity of degree n. We know that the extension $\mathbb{Q}(\omega)/\mathbb{Q}$ is Galois of degree $\varphi(n)$ (where φ is Euler's totient function); we therefore have:

Proposition. *A regular n-gon is constructible iff $\varphi(n)$ is a power of 2.*

6.8.9. Let $n = 2^r p_1^{r_1} \cdots p_l^{r_l}$ where p_i are distinct odd primes, $r \geq 0$ and $r_i \geq 1$. Then $\varphi(n) = 2^s (p_1 - 1) p_1^{r_1 - 1} \cdots (p_l - 1) p_l^{r_l - 1}$ where $s = 0$ if $r = 0$ and $s = r - 1$ if $r \geq 1$, and for $\varphi(n)$ to be a power of 2 it is necessary that for each i, $r_i = 1$ and $p_i - 1$ is a power of 2.

Prime integers of the form $2^r + 1$, $r \in \mathbb{N}$, are called *Fermat's primes*. We therefore have:

Proposition. *$\varphi(n)$ is a power of 2, and so a regular n-gon is constructible, iff $n = 2^r p_1 \cdots p_l$ where p_i are distinct Fermat's primes.*

Examples of Fermat's primes are $3 = 2^1 + 1$, $5 = 2^2 + 1$, $17 = 2^4 + 1$, $257 = 2^8 + 1$, $2^{16} + 1 = 65537$. (It is not directly related but is worth mentioning that if an integer of the form $2^r + 1$, $r \in \mathbb{N}$, is prime, then $r = 2^s$ for some integer $s \geq 0$. Indeed, if $r = km$ for an odd k, then $2^r + 1$ is divisible by $2^m + 1$: $2^r + 1 = (2^m + 1)\big(2^{(k-1)m} - 2^{(k-2)m} + \cdots - 2^m + 1\big)$.)

6.9. Linear independence of square roots of square free integers

6.9.1. Theorem. *Let $p_1, \dots, p_n$ be distinct prime integers, and let $K = \mathbb{Q}\big(\sqrt{p_1}, \dots, \sqrt{p_n}\big)$. Then $K/\mathbb{Q}$ is a free composite $\mathbb{Q}(\sqrt{p_1}) \cdots \mathbb{Q}(\sqrt{p_1})$, $[K : \mathbb{Q}] = 2^n$, and $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2^n$.*

Proof. We will prove this by induction on n: assume that the assertion holds for some n, let $K = \mathbb{Q}\big(\sqrt{p_1}, \dots, \sqrt{p_n}\big)$, and let p be a prime integer distinct from $p_1, \dots, p_n$. If $\sqrt{p} \notin K$, then $K \cap \mathbb{Q}(\sqrt{p}) = \mathbb{Q}$, both $K/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ are normal, so $K(\sqrt{p})/\mathbb{Q}$ is their free composite, and $\mathrm{Gal}\big(K(\sqrt{p})/\mathbb{Q}\big) \cong \mathbb{Z}_2^n \times \mathbb{Z}_2 = \mathbb{Z}_2^{n+1}$. So, it suffices to show that $\sqrt{p} \in K$ is impossible.

If $\sqrt{p} \in K$, then $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ is a subextension of $K/\mathbb{Q}$ of degree 2, and so, corresponds to a subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ of index 2. But $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2^n$ has $2^n - 1$ such subgroups, so K contains $2^n - 1$ quadratic subextensions, and they are all known: these are the extensions of the form $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ where $m = p_{i_1} \cdots p_{i_k}$ for some $1 \le k \le n$ and $1 \le i_1 < \cdots < i_k \le n$. So, $\mathbb{Q}(\sqrt{p}) = \mathbb{Q}(\sqrt{m})$ for some m of this form. This implies that $\sqrt{p} = c\sqrt{m}$ for some $c \in \mathbb{Q}$, so $p = c^2 m$, which is clearly impossible. ■

6.9.2. Theorem. *The set $\big\{\sqrt{m} : m$ is a square free positive integer$\big\}$ is linearly independent over $\mathbb{Q}$.*

Proof. Let Q be a finite set of square-free positive integers, and let $p_1, \dots, p_n$ be the set of all prime divisors of the elements of Q. Then every element of Q has form $p_S = \prod_{i \in S} p_i$ for some $S \subseteq \{1, \dots, n\}$. But the set $B = \big\{\sqrt{p_S} : S \subseteq \{1, \dots, n\}\big\}$ is a basis of $K = \mathbb{Q}\big(\sqrt{p_1}, \dots, \sqrt{p_n}\big)$ as a $\mathbb{Q}$-vector space, so it is linearly independent. ■

6.9.3. Let $p_1, \dots, p_n$ be distinct prime integers, let $K = \mathbb{Q}\big(\sqrt{p_1}, \dots, \sqrt{p_n}\big)$, and let $\alpha = c_1\sqrt{p_1} + \cdots + c_n\sqrt{p_n}$ for some nonzero $c_1, \dots, c_n \in \mathbb{Q}$.

Claim. *α is a primitive element of $K/\mathbb{Q}$, $K = \mathbb{Q}(\alpha)$.*

Proof. α has 2^n distinct conjugates in K, $\pm c_1\sqrt{p_1} \pm \cdots \pm c_n\sqrt{p_n}$, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n = [K : \mathbb{Q}]$, so $K = \mathbb{Q}(\alpha)$. ■

6.10. The theory of symmetric rational functions

6.10.1. A polynomial, or a rational function, $h(x_1, \dots, x_n)$ in variables $x_1, \dots, x_n$ is said to be *symmetric* if it is invariant under any permutation of $x_1, \dots, x_n$: $h(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = h(x_1, \dots, x_n)$.

6.10.2. The polynomials $s_1(x_1, \dots, x_n) = x_1 + \cdots + x_n$, $s_2(x_1, \dots, x_n) = x_1x_2 + x_1x_3 \cdots + x_{n-1}x_n$, …, $s_n(x_1, \dots, x_n) = x_1 \cdots x_n$ are called *the elementary symmetric polynomials*.

6.10.3. If a monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$, of degree n, has roots $\alpha_1, \dots, \alpha_n$, then, up to the sign, the coefficients of f are just the elementary symmetric polynomials of α_i: $a_{n-1} = -s_1(\alpha_1, \dots, \alpha_n)$, $a_{n-2} = s_2(\alpha_1, \dots, \alpha_n)$, …, $a_0 = (-1)^n s_n(\alpha_1, \dots, \alpha_n)$.

6.10.4. The fundamental theorem on symmetric polynomials says that, over any ring R, the symmetric polynomials are uniquely representable as polynomials in the elementary symmetric polynomials:

Theorem. *For every symmetric polynomial $h \in R[x_1, \dots, x_n]$ there exists a unique $g \in R[y_1, \dots, y_n]$ such that $h(x_1, \dots, x_n) = g\big(s_1, \dots, s_n\big)$.*

It follows that the ring of elementary symmetric polynomials in n variables is isomorphic to the ring of polynomials in n variables.

6.10.5. Using the Galois theory, we can obtain a slightly weaker result. Let F be a field and $n \in \mathbb{N}$. Define $K = F(x_1, \dots, x_n)$, the field of rational functions over F in variables $x_1, \dots, x_n$. The symmetric group S_n acts on K by permuting the variables x_i; the field $L = \mathrm{Fix}(S_n)$ is the field of symmetric rational functions. By Proposition 4.6.4, $[K : L] = |S_n| = n!$.

On the other hand, K is the splitting field of the so-called *generic polynomial*

$$G(x) = (x - x_1) \cdots (x - x_n) = x^n - s_1x^{n-1} + \cdots + (-1)^n s_n,$$

whose coefficients lie in the field $L' = F(s_1, \dots, s_n)$; by Theorem 2.2.6, $[K : L'] \le n!$. Since $L' \subseteq L$, we get that $L = L'$.

6.10.6. We have proved:

The fundamental theorem on symmetric functions. *For any field F and $n \in \mathbb{N}$, every symmetric rational function $h \in F(x_1, \dots, x_n)$ is representable in the form*

$$h(x_1, \dots, x_n) = g\big(s_1(x_1, \dots, x_n), \dots, s_n(x_1, \dots, x_n)\big)$$

for some $g \in F(y_1, \dots, y_n)$.

6.10.7. We have also obtained that for any field F and $n \in \mathbb{N}$, the generic polynomial $G(x) = x^n - s_1 x^{n-1} + \dots + (-1)^n s_n \in L[x]$, where $L = F(s_1, \dots, s_n)$ is the field of symmetric rational functions in n variables, has $\mathrm{Gal}(G/L) \cong S_n$.

6.10.8. As another corollary of 6.10.6 we have:

Theorem. *Let F be a field, let $f(x) = x^n + a_1 x^{n-1} + \dots + a_n \in F[x]$, and let $\alpha_1, \dots, \alpha_n$ be the roots of f (in the splitting field of f). Then for any symmetric polynomial h in n variables, $h(\alpha_1, \dots, \alpha_n) \in F$.*

---

7. Solving polynomial equations in radicals

7.1. Radical and polyradical extensions

7.1.1. Let F be a field, let $a \in F$, and $n \in \mathbb{N}$. By $\sqrt[n]{a}$ we will denote any element α of an extension of F such that $\alpha^n = a$. An extension K/F is said to be *radical* (or *simple radical*) if $K = F(\sqrt[n]{a})$ for some $a \in F$ and $n \in \mathbb{N}$.

7.1.2. An extension K/F is said to be *polyradical* (or *an extension by radicals*, or *a root extension*) if it is a tower of radical extensions.

7.1.3. Clearly, any tower and any composite of polyradical extensions is polyradical.

7.2. Cyclic and polycyclic extensions

7.2.1. An extension K/F is said to be *cyclic* if it is a Galois extension with a cyclic Galois group.

7.2.2. Theorem. *If L/F is a subextension of a cyclic extension K/F, then both K/L and L/F are cyclic.*

Proof. Subgroups and quotient groups of a cyclic group are cyclic. ■

7.2.3. A (finite, separable) extension is said to be *polycyclic* if it is a tower of cyclic extensions.

7.2.4. Theorem. (i) *A composite and a tower of polycyclic extensions is polycyclic.*

(ii) *If an extension is polycyclic then its Galois closure is polycyclic.*

Proof. (i) If K_1 and K_2 are towers of Galois extensions with Galois groups $H_1, \dots, H_n$, then their composite (assuming it is defined) is also a tower of Galois extensions with Galois groups being subgroups of H_i. So, if H_i are all cyclic, then K_1K_2 is a polycyclic extension.

If K/L and L/F are towers of cyclic extensions, then so is K/F.

(ii) If K/F is polycyclic, then the Galois closure of K/F is a composite of conjugates of K/F, which all are isomorphic to K/F and so, are polycyclic. ■

7.2.5. A group is said to be *polycyclic* if it possesses a finite subnormal series with cyclic factors. It is easy to see that a finite group is solvable iff it is polycyclic. (If a group has a subnormal series with abelian factors, then this series can be refined to a series with cyclic factors.)

7.2.6. We have:

Theorem. *A Galois extension K/F is polycyclic (=solvable) iff* $\mathrm{Gal}(K/F)$ *is a polycyclic group.*

Proof. K/F is a tower of cyclic extensions Galois extension iff $G = \mathrm{Gal}(K/F)$ has a subnormal series with cyclic factors. ■

In contrast with p-extensions, it is not however true that a non-Galois extension is polycyclic if its Galois closure is polycyclic. (Since it is not true that every subgroup of a finite polycyclic group is a member of a subnormal series with cyclic factors.)

7.3. Radical and cyclic extensions

We are now going to convince ourselves that (under certain conditions) radical and cyclic extensions are the same!

7.3.1. Theorem. *Let $n \in \mathbb{N}$, let F be a field that contains all n-th roots of unity (that is, the polynomial $x^n - 1$ splits completely in F), and let $a \in F$ be such that $\sqrt[n]{a}$ is separable over F. (This is so, for instance, if F is a perfect field, or if n is not divisible by $\operatorname{char} F$.) Then $K = F(\sqrt[n]{a})$ is a cyclic extension of F of degree dividing n.*

Proof. Let $\alpha = \sqrt[n]{a}$, $a \in F \setminus \{0\}$, and ω be a generator of the group of nth roots of 1. α is a root of the separable polynomial $x^n - a$, whose all roots are $\omega^k\alpha$, $k \in \mathbb{Z}_n$; so, all conjugates of α have this form. Since α is separable and $\omega \in F$, $K = F(\alpha)/F$ is a Galois extension; let $G = \operatorname{Gal}(K/F)$. We have a mapping $\eta\colon G \longrightarrow \mathbb{Z}_n$, $\eta(\varphi) = k$ such that $\varphi(\alpha) = \omega^k\varphi$; since φ is defined by its action on α, η is injective. For $\varphi_k, \varphi_l \in G$ such that $\eta(\varphi_k) = k$ and $\eta(\varphi_l) = l$, that is, $\varphi_k(\alpha) = \omega^k\alpha$ and $\varphi_l(\alpha) = \omega^l\alpha$, we have $\varphi_k\varphi_l(\alpha) = \varphi_k(\omega^l\alpha) = \omega^{k+l}\alpha$ (notice that G fixes ω), so η is a group homomorphism. So, G is isomorphic to a subgroup of $\mathbb{Z}_n$. ■

7.3.2. In order to show that, conversely, cyclic extensions are radical, we will need "Lagrange's resolvent", Let $n \in \mathbb{N}$, let F be a field, let $\omega \in F$ be an nth root of unity. Let K/F be a cyclic extension of degree n, and let φ be a generator of $\operatorname{Gal}(K/F)$. For $\alpha \in K$, *the Lagrange resolvent* (α, ω) is the element of K defined by

$$(\alpha, \omega) = \alpha + \omega\varphi(\alpha) + \omega^2\varphi^2(\alpha) + \cdots + \omega^{n-1}\varphi^{n-1}(\alpha).$$

7.3.3. Lemma. *In the notation of 7.3.2, for any $\alpha \in K$, $\varphi\big((\alpha, \omega)\big) = \omega^{-1}(\alpha, \omega)$, and $(\alpha, \omega)^n \in F$.*

Proof. We have

$$\varphi\big((\alpha, \omega)\big) = \varphi(\alpha) + \omega\varphi^2(\alpha) + \omega^2\varphi^3(\alpha) + \cdots + \omega^{n-1}\varphi^n(\alpha) = \omega^{-1}\big(\omega\varphi(\alpha) + \omega^2\varphi^2(\alpha) + \omega^3\varphi^3(\alpha) + \cdots + \omega^n\varphi^n(\alpha)\big) = \omega^{-1}(\alpha, \omega)$$

since $\omega^n = 1$ and $\varphi^n(\alpha) = \alpha$. Thus, $\varphi\big((\alpha, \omega)^n\big) = \omega^{-n}(\alpha, \omega)^n = (\alpha, \omega)^n$. Since φ generates $\operatorname{Gal}(K/F)$, the whole group fixes $(\alpha, \omega)^n$, so $(\alpha, \omega)^n \in F$. ■

7.3.4. In the process of proving the Fundamental theorem of the Galois theory, we had the following fact:

Lemma. *The set of automorphisms of any field is linearly independent: for any field K, any distinct $\varphi_1, \ldots, \varphi_n \in \operatorname{Aut}(K)$, and any $\beta_1, \ldots, \beta_n \in K$ not all zero, $\beta_1\varphi_1 + \cdots + \beta_n\varphi_n \neq 0$.*

Proof. Assume that the assertion is wrong and let $\beta_1\varphi_1 + \beta_2\varphi_2 + \cdots + \beta_n\varphi_n = 0$ be a minimal linear dependence relation with all $\beta_i \neq 0$. For every $\alpha \in K$ we then have

$$\beta_1\varphi_1(\alpha) + \beta_2\varphi_2(\alpha) + \cdots + \beta_n\varphi_n(\alpha) = 0. \qquad (*)$$

Let $\gamma \in K$ be such that $\varphi_1(\gamma) \neq \varphi_2(\gamma)$. (Clearly, $n \geq 2$.) For every $\alpha \in K$ we now have

$$0 = \beta_1\varphi_1(\gamma\alpha) + \beta_2\varphi_2(\gamma\alpha) + \cdots + \beta_n\varphi_n(\gamma\alpha) = \beta_1\varphi_1(\gamma)\varphi_1(\alpha) + \beta_2\varphi_2(\gamma)\varphi_2(\alpha) + \cdots + \beta_n\varphi_n(\gamma)\varphi_n(\alpha),$$

that is,

$$\beta_1\varphi_1(\gamma)\varphi_1 + \beta_2\varphi_2(\gamma)\varphi_2 + \cdots + \beta_n\varphi_n(\gamma)\varphi_n = 0. \qquad (**)$$

Subtracting $(**) - \varphi_1(\gamma)(*)$, we obtain that

$$\beta_2(\varphi_2(\gamma) - \varphi_1(\gamma))\varphi_2 + \cdots + \beta_n(\varphi_n(\gamma) - \varphi_1(\gamma))\varphi_n = 0,$$

which contradicts the minimality of $(*)$. ■

7.3.5. We can now prove:

Theorem. *Let $n \in \mathbb{N}$, let F be a field that contains a primitive nth root of unity ω, and let K/F be a cyclic extension of degree n. Then K/F is a radical extension, $K = F(\sqrt[n]{a})$ for some $a \in F$.*

(The existence of a primitive nth root of unity implies that $\operatorname{char} F \nmid n$.)

Proof. Let φ be a generator of $\operatorname{Gal}(K/F)$. By Lemma 7.3.4, the automorphisms $1, \varphi, \dots, \varphi^{n-1}$ of K/F are linearly independent, so $1 + \omega\varphi + \omega^2\varphi^2 + \dots + \omega^{n-1}\varphi^{n-1} \neq 0$, and there is $\alpha \in K$ such that $\gamma = (\alpha, \omega) \neq 0$. By Lemma 7.3.3, $a = \gamma^n \in F$. Since ω is a primitive root, $\varphi^k(\gamma) = \omega^{-k}\gamma$ are distinct for $k = 0, \dots, n-1$, so γ has n conjugates, $\deg_F \gamma = n$, and $K = F(\gamma) = F(\sqrt[n]{a})$. ■

7.3.6. Applying Theorem 7.3.5 and Theorem 7.3.1 to towers, we obtain:

Theorem. (i) *If K/F is a polycyclic extension of degree n with $\operatorname{char} F \nmid n$ and F contains a primitive nth root of unity, then K/F is polyradical.*

(ii) *If K/F is a tower of separable radical extensions, with radicals of degrees $n_1, \dots, n_k$, and for each i, F contains all n_i-th roots of unity, then K/F is polycyclic.*

7.4. Solvability of polynomials in radicals

7.4.1. An element α, algebraic over F, is *expressible by radicals* (or *can be solved for in terms of radicals*) over F if α is contained in a polyradical extension of F. A polynomial $f \in F[x]$ is said to be *solvable in radicals* (or *by radicals*) if all roots of f are expressible by radicals. Notice that if f is irreducible and one of its roots is expressible in radicals, then f is solvable in radicals.

7.4.2. The following great theorem is the main goal of the Galois theory:

Theorem. *Let F be a field and $f \in F[x]$.*

(i) *If f is separable and the group $\operatorname{Gal}(f/F)$ is solvable of order not divisible by $\operatorname{char} F$, then f is solvable in radicals.*

(ii) *If f is solvable in radicals, whose degrees, if F is not perfect, are not divisible by $\operatorname{char} F$, then $\operatorname{Gal}(f/F)$ (makes sense and) is solvable.*

Proof. (i) Let K be the splitting field of f, let ω be a primitive root of degree $n = |\operatorname{Gal}(f/F)|$. The extension $K(\omega)/F(\omega)$ is Galois, whose Galois group is a subgroup of $\operatorname{Gal}(K/F) = \operatorname{Gal}(f/F)$ and is therefore solvable. By Theorem 7.3.6, $K(\omega)/F(\omega)$ is polyradical, and since $F(\omega)/F$ is a radical extension, $K(\omega)/F$ is also polyradical. Hence, f is solvable in radicals.

(ii) Now assume that all roots of f are contained in a field K such that K/F is a tower of radical extensions where F is perfect or the degrees $n_1, \dots, n_k$ of radicals are not divisible by $\operatorname{char} F$, so that K/F is separable. Let ω be a generator of the group generated by the roots of unity of degrees $n_1, \dots, n_k$; then the extension $K(\omega)/F(\omega)$ is also polyradical, and so, polycyclic (in particular, Galois). Since $F(\omega)/F$ is also polycyclic (its Galois group is a subgroup of $\mathbb{Z}_n^*$ for some n), $K(\omega)/F$ is polycyclic. Let E/F be the Galois closure of $K(\omega)/F$, then E/F is polycylic, and so, the group $\operatorname{Gal}(E/F)$ is solvable. Let $L \subseteq E$ be the splitting field of f; then $\operatorname{Gal}(L/F)$ is a quotient group of $\operatorname{Gal}(E/F)$, so it is solvable as well. ■

7.4.3. Corollary. *If $\operatorname{char} F \neq 2, 3$, every polynomial $f \in F[x]$ of degree ≤ 4 is solvable in radicals. The general polynomial of degree ≥ 5 is not solvable in radicals.*

(This means that there is no general "symbolic" formula that allows to express the roots of a polynomial of degree ≥ 5 in radicals.)

Proof. For any polynomial f of degree n, $\operatorname{Gal}(f)$ is a subgroup of S_n. The groups S_2, S_3, S_4 are solvable, so all their subgroups are solvable, so all polynomials of degree ≤ 4 are solvable in radicals.

For $n \geq 5$, S_n is not solvable. The general polynomial of degree $n \geq 5$ has Galois group S_n and is not therefore solvable in radicals. ■

7.4.4. We see that there is no general "symbolic" formula in radicals for roots of quintic; it would however be nice to have a concrete example of a "numerical" plynomial unsolvable in radicals. The following proposition allows to construct such examples:

Proposition. *Any irreducible polynomial of degree 5 over $\mathbb{Q}$ that has three real and two non-real roots has Galois group isomorphic to S_5 and so, is unsolvable in radicals.*

(Actually, same idea allows to construct polynomials of degree p with $\operatorname{Gal} \cong S_p$ for every prime p.)

Proof. Let $f \in \mathbb{Q}[x]$ be such a polynomial and let $G = \mathrm{Gal}(f/\mathbb{Q})$. Let $\alpha \in \mathbb{C}$ be a root of f, let $K \subseteq \mathbb{C}$ be the splitting field of f. Consider G as a subgroup of S_5 via its action on the roots of f. f has two non-real complex roots, so the complex conjugation is a transposition in S_5. Since $\mathbb{Q}(\alpha) \subseteq K$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, the degree $[K : \mathbb{Q}]$ is divisible by 5, so $5 \,\big|\, |G|$. Hence, G contains an element of order 5, which may only be a 5-cycle. But (recall that) any transposition and a 5-cycle in S_5 generate S_5, so $G = S_5$. ∎

Example. $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ is irreducible, has three real and two non-real roots, so $\mathrm{Gal}(f, \mathbb{Q}) \cong S_5$, and f is unsolvable in radicals.

7.4.5. To express an element in radicals, we need first to adjoin to our basic field certain roots of unity. Applying the Galois theory to cyclotomic extensions, we can express by radicals the roots of unity themselves, like $\sqrt[3]{1} = \frac{-1+\sqrt{-3}}{2}$, $\sqrt[4]{1} = \sqrt{-1}$, $\sqrt[5]{1} = \frac{-1+\sqrt{5}}{4} + \frac{\sqrt{10+2\sqrt{5}}}{4}$, $\sqrt[6]{1} = \frac{1+\sqrt{-3}}{2}$, $\sqrt[8]{1} = \frac{\sqrt{2}+\sqrt{-2}}{2}$. (However, at least theoretically, I don't see why these expressions are better than "the radical" $\sqrt[n]{1}$.)

7.5. The alternating group and the discriminant

7.5.1. Let $f \in F[x]$ be a separable polynomial over a field F and let $\alpha_1, \ldots, \alpha_n$ be the roots of f. The Galois group $\mathrm{Gal}(f)$, through its action on the set $\{\alpha_1, \ldots, \alpha_n\}$, is identified with a subgroup of S_n. The product $\delta = \prod_{i<j}(\alpha_i - \alpha_j)$ is fixed by even permutations from S_n, and switches sign under the action of odd permutations.

7.5.2. $D = \delta^2$ is a symmetric polynomial of $\alpha_1, \ldots, \alpha_n$, so, is a polynomial in the coefficients of f, and is contained in F. It is called *the discriminant* of f, and is denoted by $\mathrm{Disc}(f)$ or $D(f)$. Notice that $D(f) = 0$ iff f has a multiple root.

(i) For a quadratic polynomial $f(x) = x^2+ax+b = (x-\alpha_1)(x-\alpha_2)$, $D(f) = (\alpha_2-\alpha_1)^2 = (\alpha_2+\alpha_1)^2-4\alpha_1\alpha_2 = a^2 - 4b$.

(ii) For a cubic polynomial $f(x) = x^3 + ax^2 + bx + c$, $D(f) = a^2b^2 + 18abc - 4b^3 - 4a^3c - 27c^2$. Replacing f by the cubic $g(x) = f(x - a/3)^2 = x^3 + px + q$ doesn't change the discriminant, $D(f) = D(g) = -4p^3 - 27q^2$.

(iii) For a quartic polynomial $f(x) = x^4+px^2+qx+r$, $D(f) = 16p^4r-4p^3q^2-128p^2r^2+144pq^2r-27q^4+256r^3$.

7.5.3. Theorem. *The Galois group* $\mathrm{Gal}(f)$ *of a separable polynomial* $f \in F[x]$ *of degree* n *is contained in the alternating group* A_n *iff* $\delta = \sqrt{D(f)} \in F$. *If* $\delta \notin F$, *then* $F(\delta)$ *is the quadratic extension of* F *fixed by* $\mathrm{Gal}(f) \cap A_n$.

Proof. $\mathrm{Gal}(f) \leq A_n$ iff all elements of $\mathrm{Gal}(f)$ fix δ, that is, iff $\delta \in F$. If this is not so, then $\mathrm{Gal}(f) \cap A_n$ is a subgroup of $\mathrm{Gal}(f)$ of index 2, so fixes a quadratic subextension L of the splitting field of f; but $F(\delta)/F$ is quadratic and fixed by $\mathrm{Gal}(f) \cap A_n$, so $L = F(\delta)$. ∎

7.5.4. Let $f \in F[x]$ be a quadratic polynomial, $f(x) = x^2 + ax + b$, over a field F of characteristic $\neq 2$. By Theorem 7.5.3, if $\sqrt{D(f)} \in F$, then $\mathrm{Gal}(f)$ is trivial, and f splits in F, otherwise $\mathrm{Gal}(f) \cong \mathbb{Z}_2$ and the splitting field of f is $F\big(\sqrt{D(f)}\big)$. (And indeed, the roots of f are $\frac{1}{2}\big(-a \pm \sqrt{D(f)}\big)$.)

7.6. The Galois group and solution in radicals of cubics

Let F be a field of characteristic $\neq 2, 3$. Let $f = x^3+a_2x^2+a_1x+a_0 \in F[x]$ be a monic irreducible cubic polynomial, let $\alpha_1, \alpha_2, \alpha_3$ be the roots of f, let $K = F(\alpha_1, \alpha_2, \alpha_3)$ be the splitting field of f, let $G = \mathrm{Gal}(f)$, and let $D = D(f)$.

7.6.1. After replacing $x + a_2/3$ by x, f takes the form $f(x) = x^3 + px + q$; this operation changes neither K, nor G, nor D.

7.6.2. G is isomorphic to a subgroup of S_3 that acts transitively on the set $\{\alpha_1, \alpha_2, \alpha_3\}$ of the roots of f; hence, either $G \cong S_3$ or $G \cong A_3 \cong \mathbb{Z}_3$. We have $G \leq A_3$ iff $\sqrt{D} \in F$, so $G \cong \mathbb{Z}_3$ in this case, and otherwise $G \cong S_3$.

7.6.3. Here are two examples of irreducible cubics over $\mathbb{Q}$ and their Galois groups:
$x^3 - 2$ has $D = -108$, so $G \cong S_3$;
$x^3 - 3x + 1$ has $D = 9^2$, so $G \cong \mathbb{Z}_3$.

7.6.4. In the case $F \subseteq \mathbb{R}$, if all roots of f are real, then $D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$ is positive; if f has one real and two non-real roots, then $D < 0$. So, if $D < 0$ then $G \cong S_3$ (and if $D > 0$ then $G \cong S_3$ or $\mathbb{Z}_3$).

7.6.5. To find a formula for the roots of f in radicals, adjoin to F a primitive 3rd root of unity $\omega = \frac{-1+\sqrt{-3}}{2}$: replace F by $F(\sqrt{-3})$ and K by $K(\sqrt{-3})$; assume that f is still irreducible. We have the tower

$$\begin{array}{c} K \\ \| 3 \\ F(\sqrt{D}) \\ \| 1 \text{ or } 2 \\ F \end{array}$$

Since K is a cyclic cubic extension of $F(\sqrt{D})$, it is radical, $K = F(\gamma)$ for some γ such that $\gamma^3 \in F(\sqrt{D})$. γ can be found as the Lagrange resolvent of one of generators of K, say, of the root α_1 of f: $\gamma = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3$. Let also $\gamma' = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3$, then $\gamma' = \tau(\gamma)$ where τ is the transposition $(2,3)$ (or rather (α_2, α_3)). We have $\gamma^3 \in F(\sqrt{D})$, that is, $\gamma^3 = a + b\sqrt{D}$ for some $a, b \in F$. Then $(\gamma')^3 = \tau(\gamma^3) = a - b\sqrt{D}$, and so, $a = \frac{1}{2}(\gamma^3 + (\gamma')^3)$ and $b = \frac{1}{2\sqrt{D}}(\gamma^3 - (\gamma')^3)$. γ^3 and $(\gamma')^3$ are fixed by any even permutation from S_3 and are switched by any odd permutation, and $\sqrt{D}$ changes sign under an odd permutation; so, a and b are symmetric polynomials in $\alpha_1, \alpha_2, \alpha_3$ and can be found: for $f(x) = x^3 + px + q$ computations give that $a = -\frac{27}{2}q$ and $b = \frac{3}{2}\sqrt{-3}$, so $\gamma^3 = -\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}$, $(\gamma')^3 = -\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}$,

$$\gamma = \sqrt[3]{-\tfrac{27}{2}q + \tfrac{3}{2}\sqrt{-3D}} \quad \text{and} \quad \gamma' = \sqrt[3]{-\tfrac{27}{2}q - \tfrac{3}{2}\sqrt{-3D}}.$$

Since $\alpha_1 + \alpha_2 + \alpha_3 = 0$, we get

$$\alpha_1 = \tfrac{1}{3}(\gamma + \gamma'), \quad \alpha_2 = \tfrac{1}{3}(\omega\gamma + \omega^2\gamma'), \quad \alpha_3 = \tfrac{1}{3}(\omega^2\gamma + \omega\gamma').$$

(Here, the cubic roots $\gamma = \sqrt[3]{\dots}$ and $\gamma' = \sqrt[3]{\dots}$ are not independent: they must satisfy

$$\gamma\gamma' = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + (\omega + \omega^2)(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = (\alpha_1 + \alpha_2 + \alpha_3)^2 - 3(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = -3p,$$

so that $\gamma' = -3p/\gamma$.) These formulas for the roots of a cubic are called *Cardano's formulas*.

7.6.6. *Casus irreducibilis.* For $f \in \mathbb{Q}[x]$, even if $D > 0$ and thus all three roots of f are real, none of them is expressible by radicals in $\mathbb{R}$ only: the radical formulas for each root will necessarily involve non-real complex numbers. Indeed, assume that a root α of f lies in a tower $K_n/K_{n-1}/\dots/K_1/\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ of real radical extensions and no root of f is contained in K_{n-1}. As we know, any real subextension of a real radical extension is also radical, so $K_{n-1}(\alpha)/K_{n-1}$ is radical, and we may assume that $K_n = K_{n-1}(\alpha)$. Since f has no roots in K_{n-1}, f is irreducible over K_{n-1}, so $[K_n : K_{n-1}] = \deg_{K_{n-1}}(\alpha) = 3$. Since $\mathbb{Q}(\alpha, \sqrt{D})/\mathbb{Q}(\sqrt{D})$ is abelian, K_n contains all roots of f and so, K_n/K_{n-1} is normal. But then $K_n \ni \omega = e^{2\pi i/3} \notin \mathbb{R}$, contradiction.

7.7. The Galois group and solution in radicals of quartics

Let F be a field of characteristic $\neq 2, 3$. Let $f = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in F[x]$ be a monic irreducible quartic polynomial with roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, let $K = F(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ be the splitting field of f, let $G = \mathrm{Gal}(f)$, and let $D = D(f)$.

7.7.1. After replacing $x + a_3/4$ by x, f takes the form $f(x) = x^4 + px^2 + qx + r$; this operation changes neither K, nor G, nor D.

7.7.2. G is a subgroup of the group S_4 acting on the set $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ of the roots of f, and the action of G on this set is transitive. Here is the list of subgroups of S_4 that act transitively:

(i) S_4 itself, of order 24;

(ii) the alternating group A_4, of order 12;

(iii) three conjugate subgroups $H_1 = \big\langle (1,3,2,4), (1,2) \big\rangle$, $H_2 = \big\langle (1,2,3,4), (1,3) \big\rangle$, $H_3 = \big\langle (1,2,4,3), (1,4) \big\rangle$ of order 8, isomorphic to D_8;

(iv) the normal subgroup $V = \big\{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\big\}$, of order 4, isomorphic to the Klein 4-group $V_4 \cong \mathbb{Z}_2^2$;

(v) and three conjugate cyclic subgroups $C_1 = \big\langle (1,3,2,4) \big\rangle$, $C_2 = \big\langle (1,2,3,4) \big\rangle$, $C_3 = \big\langle (1,2,4,3) \big\rangle$, of order 4, isomorphic to $\mathbb{Z}_4$.

7.7.3. The group S_4 is solvable and has the normal series $1 \trianglelefteq V \trianglelefteq A_4 \trianglelefteq S_4$, with $A_4/V \cong \mathbb{Z}_3$ and $S_4/A_4 \cong \mathbb{Z}_2$. Hence, G, as a subgroup of S_4, has the normal series $1 \trianglelefteq (V \cap G) \trianglelefteq (A_4 \cap G) \trianglelefteq G$, and the corresponding tower for K is $K/L/F(\sqrt{D})/F$ where $L = \mathrm{Fix}(V \cap G)$:

$$\begin{array}{c} 1 \\ \| \\ V \cap G \\ \| \\ A_4 \cap G \\ \| \\ G \end{array} \qquad\qquad \begin{array}{c} K \\ \| \\ L \\ \| \\ F(\sqrt{D}) \\ \| \\ F \end{array} \tag{7.1}$$

7.7.4. To determine L, let $\theta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$, $\theta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$, $\theta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$. (Another variant is $\theta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $\theta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$, $\theta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$.) G permutes the elements θ_i, thus the polynomial

$$R(x) = (x - \theta_1)(x - \theta_2)(x - \theta_3)$$

is contained in $F[x]$. The polynomial R is called *the cubic resolvent* of f.

Computations show that for $f(x) = x^4 + px^2 + qx + r$, $R(x) = x^3 - 2px^2 + (p^2 - 4r)x + q^2$.

Lemma. *The discriminant $D(R)$ of the cubic resolvent R of f equals the discriminant $D(f)$ of f.*

Proof. $\theta_1 - \theta_2 = \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 - \alpha_1\alpha_2 - \alpha_1\alpha_4 - \alpha_3\alpha_2 - \alpha_3\alpha_4 = \alpha_1\alpha_3 + \alpha_2\alpha_4 - \alpha_1\alpha_2 - \alpha_3\alpha_4$ $= (\alpha_1 - \alpha_4)(\alpha_3 - \alpha_2)$, similarly $\theta_1 - \theta_3 = -(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4)$ and $\theta_2 - \theta_3 = -(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4)$. Hence,

$$D(R) = \prod_{1 \le i < j \le 3} (\theta_i - \theta_j)^2 = \prod_{1 \le i < j \le 4} (\alpha_i - \alpha_j)^2 = D(f).$$

■

Hence, if f is separable, then R is separable and θ_i are all distinct. The stabilizer of θ_1 in G is the group $H_1 \cap G$, of θ_2 is $H_2 \cap G$, and of θ_3 is $H_3 \cap G$. Since $H_1 \cap H_2 \cap H_3 = V$, in the diagram (7.1) we have that $L = F(\theta_1, \theta_2, \theta_3) = \mathrm{Fix}(V \cap G)$.

7.7.5. Theorem. *Let us interpret G as a subgroup of S_4 and use notation from 7.7.2. Let R be the cubic resolvent of f.*

(i) *If R is irreducible and $\sqrt{D} \notin F$, then $G = S_4$.*

(ii) *If R is irreducible and $\sqrt{D} \in F$, then $G = A_4$.*

(iii) *If R splits completely in F, then $G = V$ (and is isomorphic to V_4).*

(iv) *If R splits over F into a linear and quadratic polynomials and f is irreducible over $F(\sqrt{D})$, then G is one of the groups H_i (and is isomorphic to D_8).*

(v) *If R splits over F into a linear and quadratic polynomials and f is reducible over $F(\sqrt{D})$, then G is one of the groups C_i (and is isomorphic to $\mathbb{Z}_4$).*

Proof. (i) In this case $\mathrm{Gal}(L/F) = G/(V \cap G) \cong S_3$. Also, since $\sqrt{D} \notin F$, $G \not\leq A_4$. From the list in 7.7.2, only S_4 has these properties.

(ii) In this case $\mathrm{Gal}(L/F) = G/(V \cap G) \cong \mathbb{Z}_3$, and since $\sqrt{D} \in F$, $G \leq A_4$. From the list in 7.7.2, only A_4 has these properties.

(iii) In this case $\mathrm{Gal}(L/F) = G/(V \cap G)$ is trivial, so $G \leq V$, so $G = V$.

(iv,v) In these cases G fixes one of θ_i, so $G \leq H_i$, so $G = H_i$ or C_i. The group $H_i \cap A_4 = V$ acts transitively on the set $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$, whereas $C_i \cap A_4 \cong \mathbb{Z}_2$ does not. Hence if f is irreducible over $F(\sqrt{D})$ (and so all α_i are conjugate over this field), then $G = H_i$; and if not, then $G = C_i$. (Notice also that $C_i \cap A_4$ is a product of two transpositions, thus in the case $G = C_i$, f splits over $F(\sqrt{D})$ into a product of two quadratic polynomials.) ■

7.7.6. When f is "biquadratic", $f = x^4 + px^2 + r$, the cubic resolvent $R(x) = (x^2 - 2px + p^2 - 4r)x$ is always reducible, so $G \ncong S_4$ or A_4. (We knew this!)

7.7.7. Here are examples of irreducible quartics, over $\mathbb{Q}$, representing all isomorphism types of Galois groups:
$x^4 - x - 1$ has $D = -283$, $R = x^3 + 4x + 1$ is irreducible, $G \cong S_4$;
$x^4 + x + 1$ has $D = 229$, $R = x^3 - 4x + 1$ is irreducible, $G \cong S_4$;
$x^4 + 8x + 12$ has $D = 576^2$, $R = x^3 - 16x + 16$ is irreducible, $G \cong A_4$;
$x^4 - 10x^2 + 1$ (the minimal polynomial of $\sqrt{2} + \sqrt{3}$) has $D = -260744$, $R = x(x + 8)(x + 12)$, $G \cong V_4$;
$x^4 + 36x + 63$ has $D = 4320^2$, $R = (x + 18)(x - 6)(x - 12)$, $G \cong V_4$;
$x^4 - 2$ has $D = -2^{11}$, $R = (x^2 + 8)x$, $x^4 - 2$ is irreducible over $\mathbb{Q}(\sqrt{-2})$, $G \cong D_8$;
$x^4 + 3x + 3$ has $D = 21 \cdot 15^2$, $R = (x - 3)(x^2 + 3x - 3)$, $G \cong D_8$;
$x^4 - 4x^2 + 2$ has $D = -19 \cdot 2^8$, $R = (x^2 + 8x + 8)x$, $G \cong \mathbb{Z}_4$;
$x^4 + 5x + 5$ has $D = 5 \cdot 55^2$, $R = (x + 5)(x^2 - 5x + 5)$, $G \cong \mathbb{Z}_4$.

7.7.8. The roots θ_i of the cubic resolvent R of f are expressible in radicals with the help of Cardano's formulas. Assume that $f(x) = x^4 + px^2 + qx + r$, then $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$, and $\theta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = -(\alpha_1 + \alpha_2)^2$, so $\alpha_1 + \alpha_2 = \sqrt{-\theta_1}$. Using this and similar equalities, we now get

$$\alpha_1 = \tfrac{1}{2}\bigl(\sqrt{-\theta_1} + \sqrt{-\theta_2} + \sqrt{-\theta_3}\bigr), \quad \alpha_2 = \tfrac{1}{2}\bigl(\sqrt{-\theta_1} - \sqrt{-\theta_2} - \sqrt{-\theta_3}\bigr),$$
$$\alpha_3 = \tfrac{1}{2}\bigl(-\sqrt{-\theta_1} + \sqrt{-\theta_2} - \sqrt{-\theta_3}\bigr), \quad \alpha_4 = \tfrac{1}{2}\bigl(-\sqrt{-\theta_1} - \sqrt{-\theta_2} + \sqrt{-\theta_3}\bigr).$$

7.8. Computation of Galois groups

7.8.1. There exist ingeneous and effective algorithms for computing Galois groups; here is one of them (which belongs to van der Waerden). Let K/F be a Galois extension, let $G = \mathrm{Gal}(K/F)$. Let $\{\alpha_1, \dots, \alpha_n\}$ be a G-invariant set of (pairwise distinct) generators of K. (If K is a splitting field of $f \in F[x]$ it is natural to take as these generators the roots of f.) Let's identify G with a subgroup of S_n acting on this set. Let $\widetilde{F} = F(x_1, \dots, x_n)$ and $\widetilde{K} = K(x_1, \dots, x_n) = \widetilde{F}(\alpha_1, \dots, \alpha_n)$, where x_i are free variables; consider the extension $\widetilde{K}/\widetilde{F}$. $\widetilde{K}/\widetilde{F}$ is Galois with $\mathrm{Gal}(tK/tF) \le \mathrm{Gal}(K/F)$; since $[\widetilde{K} : \widetilde{F}] = [K : F]$, $\mathrm{Gal}(tK/tF) = \mathrm{Gal}(K/F)$.

For each $\sigma \in S_n$ let $r_\sigma = \alpha_{\sigma(1)}x_1 + \dots + \alpha_{\sigma(n)}x_n \in \widetilde{K}[x]$; in particular, $r_1 = \alpha_1 x_1 + \dots + \alpha_n x_n$. The group S_n acts on the set $\{r_\sigma,\ \sigma \in S_n\}$ by permuting α_i:

$$\rho(r_\sigma) = \alpha_{\rho\sigma(1)}x_1 + \dots + \alpha_{\rho\sigma(n)}x_n = r_{\rho\sigma}, \quad \rho \in S_n.$$

(Or: S_n acts on $\widetilde{K}$ by permuting x_i, under which action $\rho(r_\sigma) = \sum_{i=1}^n \alpha_{\sigma(i)}x_{\rho(i)} = \sum_{i=1}^n \alpha_{\sigma\rho^{-1}(i)}x_i = r_{\sigma\rho^{-1}}$.) The conjugates of r_1 in $\widetilde{K}[x]$ are the elements $\sigma(r_1) = r_\sigma$ with $\sigma \in G$, so r_1 has $|G|$ distinct conjugates (and so, $\widetilde{K} = \widetilde{F}(r_1)$). Let $g(x) = \prod_{\sigma \in S_n}(x - r_\sigma)$; since g is invariant under all permutations of $\alpha_1, \dots, \alpha_n$, we have $g \in \widetilde{F}[x]$. Let $g = g_1 \cdots g_k$ be the factorization of g into a product of irreducible factors in $\widetilde{F}[x]$. (Finding this factorization is the computational part of the algorithm.) W.l.o.g., let $x - r_1$ be a factor of g_1, so that g_1 is the minimal polynomial of r_1. Let H be the subset of S_n such that $g_1 = \prod_{\sigma \in H}(x - r_\sigma)$; then $\{r_\sigma,\ \sigma \in H\}$ is just the set of all the conjugates of r_1, hence, $H = G$. We can also interprete H as follows: S_n acts on the set $\{g_1, \dots, g_k\}$, and $G = H$ is the stabilizer of g_1 under this action.

7.8.2. The Galois group of an integer polynomial can sometimes be found by reducing the polynomial modulo distinct primes. Let $f \in \mathbb{Z}[x]$ be a monic separable polynomial; let $D = D(f)$, then D is an integer. Let p be a prime integer not dividing D; consider the polynomial $\bar{f} = f \bmod p \in \mathbb{F}_p[x]$.

Dedekind's theorem. *As groups of permutations of the roots of f and the corresponding roots of $\bar{f}$, $\mathrm{Gal}(\bar{f}/\mathbb{F}_p)$ is a subgroup of $\mathrm{Gal}(f/\mathbb{Q})$.*

(If it is hard to calculate D to check if $p \nmid D$, this calculation can be avoided: we have $D = 0 \bmod p$ iff $\bar{f}$ is inseparable.)

Proof. Let $\alpha_1, \dots, \alpha_n$ be the roots of f. Put $R = \mathbb{Z}[\alpha_1, \dots, \alpha_n]$. p is not a unit in R. (Indeed, R is a finitely generated $\mathbb{Z}$-module, as $\mathbb{Z}$ is a ED any its submodule must also be finitely generated, but the ring $\mathbb{Z}[p^{-1}]$ is not finitely generated as a $\mathbb{Z}$-module.) So, p is contained in a maximal ideal P of R. Let $L = R/P$, then L is a field in which $p = 0$, so L is a finite extension of $\mathbb{F}_p$. L is generated by $\bar\alpha_1, \dots, \bar\alpha_n$ (the images of $\alpha_1, \dots, \alpha_n$) and is a splitting field of the polynomial $\bar f$ (the image of f in $\mathbb{F}_p[x]$). Let $G = \mathrm{Gal}(f/\mathbb{Q})$ and let $H = \{\varphi \in G : \varphi(P) = P\}$. Then H acts on L, so we have a homomorphism $\eta\colon H \longrightarrow \mathrm{Gal}(L/\mathbb{F}_p) = \mathrm{Gal}(\bar f)$. Since $D(\bar f) = D(f) \bmod p \neq 0$, $\bar f$ is separable, and the elements $\bar\alpha_i$ are distinct. Since every element of H is defined by its action on α_i, and so on $\bar\alpha_i$, η is injective and we identify H with a subgroup of $\mathrm{Gal}(\bar f)$. To prove that $H = \mathrm{Gal}(\bar f)$ it suffices to show that $|H| \geq |\mathrm{Gal}(\bar f)|$.

Let $\alpha \in R$ be such that its image $\bar\alpha \in L$ generates L, $L = \mathbb{F}_p(\bar\alpha)$. Any two of the ideals $\varphi(P)$, $\varphi \in G$, either coincide or are comaximal, thus, by the Chinese remainder theorem, there is $\beta \in R$ such that $\beta = \alpha \bmod P$ and $\beta = 0 \bmod \varphi^{-1}(P)$ for all $\varphi \in G \setminus H$. We then have $\varphi(\beta) = \varphi(\alpha) \bmod \varphi(P) = \varphi(\alpha) \bmod P$ for all $\varphi \in H$ and $\varphi(\beta) = 0 \bmod P$ for all $\varphi \in G \setminus H$. Let $g(x) = \prod_{\varphi\in G}(x - \varphi(\beta))$, then $g \in \mathbb{Q}[x]$; after replacing β by $d\beta$ (and α by $d\alpha$) for a suitable $d \in \mathbb{N}$ we may assume that $g \in \mathbb{Z}[x]$. The image of g in $\mathbb{F}_p[x]$ is $x^{|G|-|H|}\prod_{\varphi\in H}(x - \varphi(\bar\alpha))$ and is divisible by $m_{\bar\alpha}$, so $|H| \geq \deg_{\mathbb{F}_p}(\bar\alpha) = [L : \mathbb{F}_p] = |\mathrm{Gal}(\bar f)|$. ∎

7.8.3. As the group $\mathrm{Gal}(\bar f/\mathbb{F}_p)$ is cyclic and transitive on each set of conjugate roots of $\bar f$, we get:

Theorem. *For each prime integer p not dividing D, if $h_1 \cdots h_k$ is the factorization of $f \bmod p$ into irreducible factors with $n_i = \deg h_i$, $i = 1, \dots, k$, then $\mathrm{Gal}(f/\mathbb{Q})$ contains an element of the cycle type $(n_1, \dots, n_k)$.*

7.8.4. Examples. (i) Let $f = x^4 + 3x^2 - 3x - 2 \in \mathbb{Z}[x]$. Let $G = \mathrm{Gal}(f/\mathbb{Q})$. Since $f = x^4 - 2 = (x^2+x+2)(x^2+2x+2) \bmod 3$, G contains a permutation of the cycle type $(2, 2)$. Since $f = x(x^3+x+1) \bmod 2$, f contains a permutation of cycle type $(1, 3)$, that is, a 3-cycle. It also follows that f is irreducible: f hasno root since it doesn't have a root modulo 3, and f is not a product of two quadrics since it is not such a product modulo 2. Hence, $G \cong S_4$ or A_4; since (as we can compute) $D(f) < 0$, we get that $G \cong S_4$.

(ii) Let $f = x^6 + x^4 + x + 3 \in \mathbb{Z}[x]$, let $G = \mathrm{Gal}(f/\mathbb{Q})$. Then $f = (x + 1)(x^2 + x + 1)(x^3 + x + 1) \bmod 2$, $f = (x + 6)(x^5 + 5x^4 + 4x^3 + 9x^2 + x + 6) \bmod 11$, $f = (x^2 + 8x + 1)(x^2 + 9x + 10)(x^2 + 9x + 12) \bmod 13$. It follows that f is irreducible: if $f = f_1 f_2$, then taking f modulo 11 we see that f must have a linear factor, but this disagrees with the decomposition of f modulo 13. By Theorem 7.8.3, G contains permutations ρ of cycle type $(1, 2, 3)$ and σ of cycle type $(1, 5)$; σ is a 5-cycle and ρ^3 is a transposition. So, G is a transitive subgroup of S_6 that contains a 5-cycle and a transposition; it is easy to see that such a subgroup must coincide with S_6.

7.8.5. We can use Theorem 7.8.3 to construct, for every $n \in \mathbb{N}$, a polynomial $f \in \mathbb{Z}[x]$ with $\mathrm{Gal}(f/\mathbb{Q}) \cong S_n$. Let $f_2 \in \mathbb{Z}_2[x]$ be an irreducible (monic) polynomial of degree n; let $f_3 \in \mathbb{Z}_3[x]$ be a separable monic polynomial of degree n which is the product of a linear polynomial and an irreducible polynomial of degree $n - 1$; and let $f_5 \in \mathbb{Z}_5[x]$ be a separable monic polynomial of degree n that is the product of an irreducible quadratic polynomial, an irreducible polynomial of an odd degree $n - 2$ or $n - 3$, and a linear polynomial in the case n is even and ≥ 2 (in the case $n = 2$, f_5 is just a quadratic polynomial). Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree n such that $f = f_2 \bmod 2$, $f = f_3 \bmod 3$, and $f = f_5 \bmod 5$; it exists by the Chinese remainder theorem. (Say, $f = -15\tilde f_2 + 10\tilde f_3 + 6\tilde f_5$, where $\tilde f_p \in \mathbb{Z}[x]$ are such that $f_p = \tilde f_p \bmod p$, $p = 2, 3, 5$.) Let $G = \mathrm{Gal}(f/\mathbb{Q})$. Since f_2 is irreducible, f is irreducible. By Theorem 7.8.3 with $p = 3$, G contains an $(n - 1)$-cycle, and with $p = 5$, G contains a product $\tau\rho$ of a transposition τ and a m-cycle ρ with an odd m; then $(\tau\rho)^m = \tau$ is also in G. A simple lemma says that if a subgroup of S_n is transitive and contains an $(n - 1)$-cycle and a transposition then it coincides with S_n; so, $G = S_n$.

7.8.6. The discriminant of a polynomial (which is so important for determining its Galois group) can sometimes be found with the help of a *resultant*. For two polynomials $f, g \in F[x]$, $f(x) = a(x - \alpha_1) \cdots (x - \alpha_n)$ and $g(x) = b(x - \beta_1) \cdots (x - \beta_m)$, *the resultant* of f and g is $\mathrm{Res}(f, g) = a^m b^n \prod_{i,j}(\alpha_i - \beta_j)$. Since $\mathrm{Res}(f, g)$ is invariant under any permutation of α_i-s and of β_j-s, we have $\mathrm{Res}(f, g) \in F$. Clearly, $\mathrm{Res}(f, g) = 0$ iff f and g have a common root.

Directly from the definition, $\mathrm{Res}(f, g) = a^m \prod_{i=1}^n g(\alpha_i) = (-1)^{nm} b^n \prod_{j=1}^m f(\beta_j)$. In particular, if f is linear, $f(x) = a(x - \alpha)$, then $\mathrm{Res}(f, g) = a^m g(\alpha)$.

7.8.7. We have:

Lemma. *If f is a monic polynomial of degree n, then $D(f) = (-1)^{n(n-1)/2}\operatorname{Res}(f, f')$.*

Proof. Let $f(x) = \prod_{i=1}^{n}(x-\alpha_i)$, then $f'(x) = \sum_{i=1}^{n}\prod_{j\neq i}(x-\alpha_j)$, and for every i, $f'(\alpha_i) = \prod_{j\neq i}(\alpha_i-\alpha_j)$. So,

$$\operatorname{Res}(f,f') = \prod_{i=1}^{n} f'(\alpha_i) = \prod_{i=1}^{n}\prod_{j\neq i}(\alpha_i-\alpha_j) = \prod_{i\neq j}(\alpha_i-\alpha_j) = (-1)^{n(n-1)/2}\prod_{i<j}(\alpha_i-\alpha_j)^2 = (-1)^{n(n-1)/2}D(f).$$

■

7.8.8. From the identity $\operatorname{Res}(f,g) = (-1)^{nm}b^n\prod_{j=1}^{m} f(\beta_j)$ it follows that if f_1 is a polynomial of degree n_1 such that $f_1 = f \bmod g$, then $\operatorname{Res}(f,g) = (-1)^{(n-n_1)m}b^{n-n_1}\operatorname{Res}(f_1,g)$.

7.8.9. Let's use 7.8.8 to compute the discriminant $D(f)$ for polynomials of the form $f = x^n + ax + b$. We have $f'(x) = nx^{n-1} + a$, so $f(x) = \frac{1}{n}xf'(x) + \frac{n-1}{n}ax + b$, so

$$\begin{aligned} D(f) &= (-1)^{n(n-1)/2}\operatorname{Res}(f,f') = (-1)^{n(n-1)/2}n^{n-1}(-1)^{(n-1)^2}\operatorname{Res}\big(\tfrac{n-1}{n}ax+b, f'\big) \\ &= (-1)^{(n+2)(n-1)/2}n^{n-1}\big(\tfrac{n-1}{n}a\big)^{n-1}f'\big(-\tfrac{bn}{a(n-1)}\big) = (-1)^{(n+2)(n-1)/2}n^{n-1}\big(\tfrac{n-1}{n}a\big)^{n-1}\Big(n\big(-\tfrac{bn}{a(n-1)}\big)^{n-1}+a\Big) \\ &= (-1)^{n(n-1)/2}n^nb^{n-1} + (-1)^{(n+2)(n-1)/2}(n-1)^{n-1}a^n. \end{aligned}$$

For $n = 5$ this is $D(f) = 5^5b^4 + 4^4a^5$.

---

8. Introduction to transcendental extensions

The theory of transcendental extensions resembles the theory of modules over integral domains, with linear dependence replaced by algebraic (polynomial) dependence. Let F be a field.

8.0.1. A set A of elements of an extension K/F is said to be *algebraically dependent over F* if for some $\alpha_1,\dots,\alpha_k \in A$ there is a nonzero polynomial $f \in F[x_1,\dots,x_k]$ such that $f(\alpha_1,\dots,\alpha_k) = 0$; A is said to be *algebraically independent* otherwise.

8.0.2. If a set A is algebraically dependent, $f(\alpha_1,\dots,\alpha_k) = 0$ with $f \in F[x_1,\dots,x_k]\setminus F[x_1,\dots,x_{k-1}]$, then α_k is algebraic over $F(\alpha_1,\dots,\alpha_{k-1})$. The converse is also true, and we see that A is algebraically dependent iff there is $\alpha \in A$ such that α is algebraic over $F\big(A\setminus\{\alpha\}\big)$.

8.0.3. Let K/F be an extension; a maximal algebraically independent over F subset B of K is called *a transcendence base* of K/F. A set $B \subseteq K$ is a transcendence base of K/F iff $K/F(B)$ is an algebraic extension.

8.0.4. Using Zorn's lemma, we can easily prove:

Theorem. *For any extension K/F, a transcendence base of K/F exists.*

8.0.5. We can also prove that all transcendence bases of K/F have the same cardinality. (We need "a polynomial" analogue of the replacement theorem to do this.) The cardinality of a transcendence base of K/F is called *the transcendence degree* of K/F.

8.0.6. An extension K/F is said to be *purely transcendental* if it has a transcendence base B such that $K = F(B)$. In this case, K is isomorphic to the field of rational functions in variables x_α, $\alpha \in B$.

8.0.7. We obtain that every extension K/F is a tower, $K/L/F$, where L/F is purely transcendental and K/L is algebraic.