Fields and the Galois theory

April 22, 2020

Table of Contents

1. Algebraic extensions of fields 2
   1.1. Fields, prime subfield, characteristic 2
   1.2. Extensions and subextensions 2
   1.3. Finite extensions 3
   1.4. Simple extensions 4
   1.5. Towers of simple extensions 4
   1.6. A composite of two finite extensions 5
   1.7. Algebraic extensions 5
   1.8. Quadratic and biquadratic extensions 5
   1.9. Homomorphisms of extensions 6
2. Adjoining of roots of polynomials 6
   2.1. Adjoining a root of an irreducible polynomial 6
   2.2. Conjugate elements 6
   2.3. Splitting fields 7
   2.4. Algebraic closure 7
   2.6. Separable polynomials and extensions and the Frobenius endomorphism 8
3. Cyclotomic extensions and finite fields 8
   3.1. Cyclotomic fields 8
   3.2. Finite fields 9
4. Galois extensions and the Galois theorem 9
   4.1. Embeddings and conjugate subextensions 9
   4.2. Normal extensions 10
   4.3. Galois extensions 10
   4.4. Composites and towers of separable extensions 11
   4.5. Examples of Galois groups 11
   4.6. The fundamental Galois theorem 12
   4.7. Examples of diagrams of subextensions and the corresponding Galois groups 13
5. Composites and towers of Galois extensions 13
   5.1. Change of the basic field of a Galois extension 13
   5.2. The composite of two extensions of which one is Galois 13
   5.3. The composite of two Galois extensions 14
   5.4. Free composites of Galois extensions 14
   5.5. Composites and the Galois closure of towers of Galois extensions 15
6. Some applications of the Galois theory 16
   6.1. More methods of finding the minimal polynomial of an algebraic element 16
   6.2. The norm of an algebraic element 16
   6.3. Abelian extensions 16
   6.4. Subextensions of the real radical extension $F(\sqrt[n]{a})/F$, $a > 0$, and the Galois group of $x^n - a$ 16
   6.5. The theorem on a primitive element 17
   6.6. $p$-extensions 17
   6.7. The fundamental theorem of algebra 17
   6.8. Constructions with ruler and compass 17
   6.9. Linear independence of square roots of square free integers 18
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) $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, 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 $F(x_1, \ldots, x_n)$ 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 $P \cong \mathbb{Z}/p\mathbb{Z}$ for some prime $p \in \mathbb{N}$, and $P$ is a field isomorphic to $\mathbb{F}_p$; it is called the prime subfield of $F$. We say that $F$ has characteristic $p$ in this case, and 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.

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 $\frac{K}{F}$.

(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 $S$,

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

If $S$ is finite, $S = \{ \alpha_1, \ldots, \alpha_n \}$, we write $F[\alpha_1, \ldots, \alpha_n]$ 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 $F[S]$: $F(S) = \left\{ \frac{\alpha}{\beta} : \alpha, \beta \in F[S], \beta \neq 0 \right\}$.

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, $S = \{\alpha_1, \ldots, \alpha_n\}$, then we write $F(\alpha_1, \ldots, \alpha_n)$ for $F(S)$.

1.2.6. A sequence $K_1/K_0, K_1/K_0 \cap K_0, \ldots$ 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:

```
    L_1L_2
   /    \  \
L_1    L_2
  / \    / \ \
L_1 \cap L_2
```

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

```
    K
   /    \  \
L_1    L_2
  / \    / \ \
L_1 \cap L_2
```

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 $L_1 \cap L_2$.

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: $\frac{K}{F}$.

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 $CB = \left\{ \gamma\beta : \gamma \in C, \beta \in B \right\}$ is a basis of $K$ 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 $[K : L] | [K : F]$ and $[L : F] | [K : F]$.
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 $\alpha \in F$. We then have an $F$-algebras homomorphism $\varphi: F[x] \rightarrow K$ sending $x$ to $\alpha$ 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 $\varphi: F[x] \rightarrow K$ be the homomorphism that maps $x$ to $\alpha$. 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, $K = \{f(\alpha), f \in K[x], \deg f \leq n - 1\}$ 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 $\alpha$ is algebraic over $F$.
(ii) Call the irreducible polynomial $p$ the minimal polynomial of $\alpha$ and denote it by $m_{\alpha,F}$ or just $m_{\alpha}$. The minimal polynomial $m_{\alpha,F}$ of $\alpha$ 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 $m_{\alpha} \mid f$. $m_{\alpha}$ is the only irreducible polynomial such that $m_{\alpha}(\alpha) = 0$.
(iii) Call the degree of $m_{\alpha}$ (which is also the degree $[K : F]$) the degree of $\alpha$ 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 $\alpha$ is transcendental over $F$.

1.4.4. If $K/F$ is a finite extension then for every $\alpha \in K$, $\deg_{F} \alpha \mid [K : F]$.

1.4.5. Let $K/F$ be a finite extension and let $\alpha \in K$. Here are some methods of funding the minimal polynomial $m_{\alpha,F}$ of an element $\alpha$ 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 $\alpha$ in coordinates with respect to a basis of $K$ over $F$, and find the minimal linear dependence relation between them.
(iii) The action of $\alpha$ 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 $\alpha$) is $p_{1}$.
(iv) It follows from (iii) that the characteristic polynomial $c_{T}$ of $T$ is $m_{\alpha}^{d}$. So, $m_{T}$ is the irreducible polynomial for which $c_{T} = m_{\alpha}^{d}$.
(iv) See also subsection 6.1 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 $\alpha$ is algebraic over $L$ as well, and $m_{\alpha,L} \mid m_{\alpha,F}$, so $\deg m_{\alpha,L} \leq \deg m_{\alpha,F}$.

1.5.3. Theorem. If $K/F$ is an extension and $\alpha_{1}, \ldots, \alpha_{n} \in K$ are algebraic over $F$, then $F(\alpha_{1}, \ldots, \alpha_{n}) = F(\alpha_{1}, \ldots, \alpha_{n})$, and we have

$$[F(\alpha_{1}, \ldots, \alpha_{n}) : F] = \prod_{i=1}^{n} \deg F(\alpha_{1}, \ldots, \alpha_{i-1}) \alpha_{i} \leq \prod_{i=1}^{n} \deg_{F} \alpha_{i}$$
1.6. A 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 \( [L_1L_2 : F] \leq [L_1 : F] \cdot [L_2 : F] \). If, as an \( F \)-vector spaces, \( L_1 \) is spanned by a set \( \{\alpha_1, \ldots, \alpha_n\} \) and \( L_2 \) by a set \( \{\beta_1, \ldots, \beta_m\} \), then \( L_1L_2 \) is spanned by the set \( \{\alpha_i\beta_j, \ i = 1, \ldots, n, \ j = 1, \ldots, m\} \).

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

\[
\begin{array}{c}
L_1L_2 \\
 L_1 \\
L_2 \\
L_1 \cap L_2.
\end{array}
\]

we have \( nm = n'm, \ n' \leq n \), and \( m' \leq m \). 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 \( L_1 \otimes_F L_2 \rightarrow L_1L_2 \) is surjective. In the case \( [L_1L_2 : F] = [L_1 : F] \cdot [L_2 : F] \), this is an isomorphism, and if \( \{\alpha_1, \ldots, \alpha_n\} \) is a basis of \( L_1 \) over \( F \) and \( \{\beta_1, \ldots, \beta_m\} \) is a basis of \( L_2 \), then \( \{\alpha_i\beta_j, \ i = 1, \ldots, n, \ j = 1, \ldots, m\} \) is a basis of \( L_1L_2 \).

1.7. Algebraic extensions

1.7.1. An extension \( K/F \) is said to be algebraic if every \( \alpha \in K \) is algebraic over \( F \), and is called transcendental otherwise.

1.7.2. Theorem. Any finite extension is algebraic. An algebraic extension is finite iff it is finitely generated.

1.7.3. Theorem. Towers and composites of algebraic extensions are algebraic: 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.

1.7.4. Theorem. If an extension \( K/F \) is generated by algebraic elements, then it is algebraic.

1.7.5. Let \( K/F \) be an extension. Then the set \( E = \{\alpha \in K : \alpha \text{ is algebraic over } F\} \) is a subfield of \( K \), and \( E/F \) is the maximal algebraic subextension of \( K/F \). Any element \( \alpha \in K \setminus E \) is transcendental over \( E \).

1.8. Quadratic and biquadratic extensions

Let \( F \) be a field with char \( F \neq 2 \).

1.8.1. Any quadratic extension \( K/F \) has form \( K = F(\sqrt{d}) \) for some \( d \in F \). An element \( \alpha \in K \) satisfies \( \alpha^2 \in F \) iff \( \alpha \in F \) or \( \alpha \in F\sqrt{d} \) (that is, \( \alpha = a\sqrt{d} \) for some \( a \in F \)).

1.8.2. A quartic extension \( K/F \) is called biquadratic if it is a composite of two quadratic extensions: \( K = F(\sqrt{d_1}, \sqrt{d_2}) \) for some \( d_1, d_2 \in F \) such that \( \sqrt{d_1}, \sqrt{d_2}, \sqrt{d_1d_2} \notin F \). The set \( \{1, \sqrt{d_1}, \sqrt{d_2}, \sqrt{d_1d_2}\} \) is a basis of \( K \) over \( F \).

1.8.3. Let \( K/F \) be biquadratic, \( K = F(\sqrt{d_1}, \sqrt{d_2}) \). 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 \( \alpha \in F\sqrt{d_1d_2} \). Since every nontrivial proper subextension of a biquadratic extension must be quadratic, here is the complete diagram of subextensions of \( K/F \):

\[
\begin{array}{c}
K = F(\sqrt{d_1}, \sqrt{d_2}) \\
 F(\sqrt{d_1}) \supseteq F(\sqrt{d_1}) \supseteq F(\sqrt{d_1}) \\
 F(\sqrt{d_2}) \supseteq F(\sqrt{d_2}) \supseteq F(\sqrt{d_2}) \\
 F(\sqrt{d_1d_2}) \supseteq F(\sqrt{d_1d_2}) \supseteq F(\sqrt{d_1d_2})
\end{array}
\]
1.9. Homomorphisms of extensions

1.9.1. If \( \varphi: A_1 \to A_2 \) is a mapping and \( B \subseteq A_1 \cap A_2 \), we say that \( \varphi \) fixes \( B \) if \( \varphi(a) = a \) for every \( a \in B \).

1.9.2. If \( K_1/F \) and \( K_2/F \) are two extensions of a field \( F \), a homomorphism \( K_1/F \to K_2/F \), or a homomorphism \( K_1 \to K_2 \) over \( F \), is a homomorphism \( \varphi: K_1 \to K_2 \) that fixes \( F \\
\begin{array}{c}
K_1 \\
\varphi \\
\downarrow
\end{array}
\begin{array}{c}
F \\
\end{array}
\begin{array}{c}
K_2.
\end{array}
\]

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

---

2. Adjoining of roots of polynomials

2.1. Adjoining a root of an irreducible polynomial

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 \( \alpha \) is a root of \( f \). An element \( \alpha \in K \) is a root of some nonzero \( f \in F[x] \) iff \( \alpha \) is algebraic over \( F \) and \( m_{\alpha,F} \) divides \( f \). A nonzero polynomial cannot have more than \( \deg f \) roots in any extension of \( F \).

2.1.2. Theorem. Let \( K_1/F \) and \( K_2/F \) be two extensions of a field \( F \), and assume that algebraic elements \( \alpha_1 \in K_1 \) and \( \alpha_2 \in K_2 \) have the same minimal polynomial: \( m_{\alpha_1,F} = m_{\alpha_2,F} = p \in F[x] \). Then \( F(\alpha_1)/F \cong F(\alpha_2)/F \) under an isomorphism that maps \( \alpha_1 \) to \( \alpha_2 \\
\begin{array}{c}
F(\alpha_1) \\
\sim \\
\downarrow
\end{array}
\begin{array}{c}
F(\alpha_2),
\alpha_1 \leftrightarrow \alpha_2.
\end{array}
\]

Conversely, if \( \varphi: K_1/F \to K_2/F \) 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, \( m_{\alpha_2,F} = m_{\alpha_1,F} \).

2.1.3. Now let \( F \) be a field and \( p \in F[x] \) be a (nonconstant) irreducible polynomial. Then \( K = F[x]/(p) \) is a field. Let \( \alpha \in K \) be the class of \( x \) modulo \( p \) in \( K \), then \( p \) is the minimal polynomial of \( \alpha \) over \( F \). We therefore have the following result:

Theorem. For any irreducible polynomial \( p \) over a field \( F \) there exists a simple extension \( K = F(\alpha) \) of \( F \) such that \( p \) is the minimal polynomial of \( \alpha \). Such an extension is unique up to an isomorphism that maps \( \alpha \) to another root of \( p \).

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

2.1.5. Any (not necessarily irreducible) nonconstant polynomial \( f \in F[x] \) has a root in some extension of \( F \). (This is a root of one of its irreducible factors.) Two polynomials \( f_1, f_2 \in F[x] \) are relatively prime iff they don’t have a common root in every extension of \( F \).

2.2. Conjugate elements

2.2.1. 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 \( m_{\alpha_1,F} = m_{\alpha_2,F} \).

An algebraic over \( F \) element \( \alpha \in K \) has at most \( \deg_F \) \( \alpha \) conjugates in \( K \), counting itself.

2.2.2. If \( L/F \) is a subextension of an extension \( K/F \), then the set of conjugates of an element \( \alpha \in K \) over \( L \) is a subset of the set of conjugates of \( \alpha \) over \( F \).
2.3. Splitting fields

2.3.1. If \( \varphi: F_1 \rightarrow F_2 \) is an isomorphism of fields, then \( \varphi \) naturally extends, by putting \( \varphi(x) = x \), to an isomorphism \( F_1[x] \rightarrow F_2[x] \) of the rings of polynomials over \( F_1 \) and \( F_2 \).

Theorem 2.1.2 has the following formal generalization:

Theorem. Let \( \varphi: F_1 \rightarrow F_2 \) be an isomorphism of two fields, let \( p_1 \) be an irreducible polynomial over \( F_1 \), let \( p_2 = \varphi(p_1) \), let \( \alpha_1 \) be a root of \( p_1 \) and \( \alpha_2 \) be a root of \( p_2 \). Then \( \varphi \) extends to an isomorphism \( F_1(\alpha_1) \rightarrow F_2(\alpha_2) \) that maps \( \alpha_1 \) to \( \alpha_2 \):

\[
\varphi: F_1(\alpha_1) \cong F_2(\alpha_2), \quad \alpha_1 \leftrightarrow \alpha_2.
\]

Conversely, if \( \varphi: K_1 \rightarrow K_2 \) 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 \( m_{\alpha_2,F_2} = \varphi(m_{\alpha_1,F_1}) \).

2.3.2. Let \( K \) be a field, and let \( f \in K[x] \) be a polynomial of degree \( n \geq 1 \). We say that \( f \) completely splits in \( K \) if \( f(x) = a(x-\alpha_1) \cdots (x-\alpha_n) \) for some \( a, \alpha_1, \ldots, \alpha_n \in K \), this means that “all roots of \( f \) are in \( K \)”:\n
\[
f \text{ has } n \text{ roots in } K \text{ counting with multiplicity, and no additional roots of } f \text{ appear in any extension of } K.
\]

2.3.3. 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 \( f \) completely splits in \( K \) and \( K \) is generated by the roots of \( f \). (Informally, \( K \) is obtained from \( F \) by adjoining all roots of \( f \).)

2.3.4. 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 \((\deg f)!\).  

2.3.5. The uniqueness part of Theorem 2.3.4 can be formally generalized:

Theorem. Let \( \varphi: F_1 \rightarrow F_2 \) 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 splitting fields of \( f_1 \) and \( f_2 \) respectively. Then \( \varphi \) extends to an isomorphism \( K_1 \rightarrow K_2 \) that maps roots of \( f_1 \) to roots of \( f_2 \):

\[
\varphi: K_1 \cong K_2 \\
\varphi: F_1 \cong F_2.
\]

2.3.6. Let \( \alpha \) be an algebraic element over a field \( F \). Then the splitting field \( K \) of the minimal polynomial of \( \alpha \) “contains all conjugates of \( \alpha \)”, in the sense that if \( E \) is any extension of \( K \), all conjugates of \( \alpha \) in \( E \) are contained in \( K \).

2.4. Algebraic closure

2.4.1. A field \( K \) is said to be algebraically closed if every nonconstant polynomial from \( K[x] \) has a root in \( K \); in this case, every polynomial from \( K[x] \) completely splits in \( K \). A field is algebraically closed iff it has no nontrivial algebraic extensions.

2.4.2. 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 \( K \). The algebraic closure of \( F \) is often denoted by \( \overline{F} \).

2.4.3. Theorem. For every field \( F \), the algebraic closure of \( F \) is algebraically closed.

2.4.4. Theorem. For every field \( F \), the algebraic closure of \( F \) exists, and is unique up to isomorphism over \( F \).

2.5. Proposition. If \( K/F \) is an extension where \( K \) is algebraically closed, then for any algebraic extensions \( L/F \) there exists an embedding \( L/F \rightarrow K/F \).

2.5.1. Theorem. Every algebraic extension of a field \( F \) is isomorphic to a subextension of the algebraic closure of \( F \).
2.6. Separable polynomials and extensions and the Frobenius endomorphism

2.6.1. 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 \( n \) is separable iff \( f \) has \( n \) distinct roots in its splitting field.

2.6.2. A polynomial \( f \) is separable iff it has no common roots with its derivative \( f' \), that is, iff \( f \) and \( f' \) are relatively prime.

2.6.3. Let \( f \) be an irreducible polynomial over a field \( F \). Then \( f \) is inseparable iff \( f' = 0 \). If \( \text{char} \, F = 0 \), every irreducible polynomial over \( K \) is separable. If \( \text{char} \, F = p \neq 0 \), then \( f \) is inseparable iff \( f(x) = g(x^p) \) for some \( g \in F[x] \).

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

2.6.5. An extension \( K/F \) is said to be separable if every \( \alpha \in K \) is separable over \( F \).

2.6.6. Non-separable extensions are said to be inseparable. An example of an inseparable extension is \( \mathbb{F}_p(t)/\mathbb{F}_p(t^p) \): the polynomial \( x^p - tp \in \mathbb{F}_p(t^p)[x] \) 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 \( p \).

2.6.7. 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.

2.6.8. A field \( F \) is said to be perfect if any algebraic extension of \( F \) is separable.

2.6.9. Theorem. Any field of characteristic zero is perfect. A field \( F \) of characteristic \( p \) is perfect iff for every \( a \in F \) there exists \( b \in F \) such that \( b^p = a \).

2.6.10. Every finite field is perfect.

2.6.11. Let \( F \) be a field of characteristic \( p \). The mapping \( \phi: F \to F \) defined by \( \phi(a) = a^p \) is an endomorphism of \( F \), called the Frobenius endomorphism. By Theorem 2.6.9, \( F \) is a perfect field iff its Frobenius endomorphism is surjective, that is, is an automorphism.

3. Cyclotomic extensions and finite fields

3.1. Cyclotomic fields

Let \( F \) be a field.

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

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

3.1.3. The \( n \)th roots of unity form, under multiplication, a cyclic group of order \( m \) dividing \( n \).

3.1.4. The splitting field of the polynomial \( x^n - 1 \in F[x] \) is called the \( n \)th cyclotomic extension of \( F \); the \( n \)-th cyclotomic extension of \( \mathbb{Q} \) is called the \( n \)th cyclotomic field.

3.1.5. Let \( K \) be the \( n \)th cyclotomic extension of \( F \), and let \( G \) be the group of roots of unity of degree \( n \) in \( K \). If \( \text{char} \, F = 0 \) or \( \text{char} \, F = p \) with \( p \nmid n \), then \( |G| = n \); if \( \text{char} \, F = p \) and \( n = p^m \), \( (m, p) = 1 \), then the roots of unity of degree \( n \) are the roots of unity of degree \( m \).

Let us assume below that \( \text{char} \, F = 0 \) or \( \text{char} \, F \nmid n \). Then the set of generators of \( G \) is the set of primitive \( n \)th roots of unity in \( K \). If \( \omega \) is a primitive \( n \)th root of unity, then all other \( n \)th roots of unity have form \( \omega^k \), \( k = 0, 1, \ldots, n - 1 \), and primitive \( n \)th roots of unity are the elements \( \omega^k \) for \( k \) coprime with \( n \); there are exactly \( \varphi(n) \) of them, where \( \varphi \) is Euler’s function. In particular, we have \( K = F(\omega) \).

3.1.6. The \( n \)th roots of unity over \( \mathbb{Q} \) are the complex numbers \( e^{2k\pi i/n} \), \( k = 0, 1, \ldots, n - 1 \). \( n \)th roots of unity over \( \mathbb{Q} \) are the complex numbers \( e^{2\pi i/n} \) is a primitive \( n \)th root of unity.
3.1.7. Let $P_n$ be the set of primitive $n$th roots of unity over $F$ (contained in the cyclotomic extension of $F$): $P_n = \{\omega^k : 1 \leq k \leq n-1, (k,n) = 1\}$, where $\omega$ is any primitive $n$th root of unity. The polynomial $\Phi_n(x) = \prod_{\alpha \in P_n} (x - \alpha)$, of degree $\varphi(n)$, is called the $n$th cyclotomic polynomial.

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

3.1.9. Corollary. For every $n \in \mathbb{N}$, $\Phi_n$ has integer coefficients.

3.1.10. $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$, $\Phi_4(x) = x^2 + 1$, $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, $\Phi_6(x) = x^2 - x + 1$. $\Phi_{105}$ is the first cyclotomic polynomial having a coefficient distinct from $\pm 1$.

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

3.1.12. Theorem. For every $n \in \mathbb{N}$, $\Phi_n$ is irreducible in $\mathbb{Z}[x]$. Thus, all primitive $n$th roots of unity over $\mathbb{Q}$ are conjugate (over $\mathbb{Q}$).

3.1.13. Corollary. For every $n \in \mathbb{N}$, the $n$th 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 $p = \text{char} \ K$ and $n = [K : \mathbb{F}_p]$.

3.2.2. 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 $f(x) = x^p - x \in \mathbb{F}_p[x]$, and consists of the roots of this polynomial.

This field is denoted by $\mathbb{F}_{p^n}$.

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

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

(ii) in $\mathbb{F}_{p^n}[x]$, there exists an irreducible polynomial of degree $n$.

3.2.4. Lemma. If $d, n \in \mathbb{N}$ are such that $d \mid n$, then for any $r \in \mathbb{N}$, $(x^d - 1)^r = (x^n - 1)^r$.

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 contains no other subfields.

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

3.2.6. Theorem. For any prime integer $p$ and $n \in \mathbb{N}$, every element of $\mathbb{F}_{p^n}$ is a root of an irreducible polynomial of degree $d \mid n$, and is a generator of the subfield $\mathbb{F}_{p^d}$ of $\mathbb{F}_{p^n}$. The product of all irreducible polynomials from $\mathbb{F}_p[x]$ whose degree divides $n$ equals $x^p - x$. If $\psi(n)$ is the number of irreducible polynomials of degree $n$ in $\mathbb{F}_p[x]$, then $\sum_{d|n} d\psi(d) = p^n$.

3.2.7. The fields $\mathbb{F}_{p^n}$ form a nested sequence, $\mathbb{F}_p \subseteq \mathbb{F}_{p^2} \subseteq \cdots $; the algebraic closure of $\mathbb{F}_p$ is the union of this sequence, $\mathbb{F}_p = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$.

4. Galois extensions and the Galois theorem

4.1. Embeddings and conjugate subextensions

4.1.1. Let $K/F$ and $E/F$ be two extensions. A homomorphism $K/F \rightarrow E/F$ (that is, a homomorphism $K \rightarrow E$ 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 $K/F \rightarrow K/F$ 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 $\text{Aut}(K/F)$.

Any embedding of a finite extension $K/F$ into itself is an automorphism of $K/F$.

4.1.3. 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 an element $\alpha' \in E$ conjugate to $\alpha$ over $F$. 
4.1.4. Let \( E/F \) be an extension, and let \( \alpha \) be an element algebraic over \( F \). The set of embeddings \( F(\alpha)/F \to E/F \) is in one-to-one correspondence with the set of roots of the minimal polynomial \( m_{\alpha,F} \) of \( \alpha \) in \( E \): each embedding \( \varphi: F(\alpha)/F \to E/F \) 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 \( F \).

4.1.5. Here is a generalization of 4.1.4. Let \( \psi: F_1 \to E \) be a homomorphism of fields, let \( F_2 = \varphi(F_1) \), and so, there is an embedding \( \psi: F_1(\alpha) \to E \) extending \( \varphi \) (that is, with \( \varphi|_{F_1} = \varphi \)), we have \( 0 = \varphi(f_1(\alpha)) = \varphi(f_1)(\varphi(\alpha)) = f_2(\varphi(\alpha)) \), so \( \psi \) maps \( \alpha \) to a root \( \alpha' \) of \( f_2 \), and is defined by \( \alpha' \). Thus, the set of homomorphisms \( \psi: F_1(\alpha) \to E \) extending \( \varphi \) is in one-to-one correspondence with the set of roots of \( f_2 \) in \( E \). There are at most \( \deg_{F_1} \alpha \) such homomorphisms of \( F_1 \) to \( E \); there are exactly \( \deg_{F_1} \alpha \) such homomorphisms iff \( f_2 \) is separable and completely splits in \( E \).

Note also that if \( \varphi \) is a homomorphism over a subfield \( F \) of \( F_1 \) and \( F_2 \) (that is, with \( \varphi|_F = \text{Id}_F \)) and \( f = m_{\alpha,F} \), then for each \( \alpha \) in \( F_1 \) extending \( \varphi \), there is a homomorphism \( \psi: F_1(\alpha) \to E \) extending \( \varphi \), and so, there is an embedding \( \psi: F_1(\alpha) \to E \) extending \( \varphi \).

4.1.6. **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 \( K/F \to E/F \). 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 \( E \), then there are exactly \( n \) embeddings \( K/F \to E/F \), and in this case, for every element \( \alpha \in K \), \( m_{\alpha,F} \) is separable and completely splits in \( E \).

4.1.7. If \( K/F \) is a subextension of \( E/F \) and \( \varphi: K/F \to E/F \) is an embedding, then the extension \( \varphi(K)/F \) is said to be **conjugate** to \( K/F \). By Theorem 4.1.6, a subextension of degree \( n \) may have at most \( n \) conjugates in an extension \( E/F \).

4.2. **Normal extensions**

4.2.1. An algebraic extension \( K/F \) is said to be **normal** if for any \( \alpha \in K \) “all conjugates of \( \alpha \) are in \( K \), that is, the minimal polynomial of \( \alpha \) over \( F \) completely splits in \( K \). Equivalently, \( K/F \) is normal if any irreducible polynomial from \( F[x] \) that has a root in \( E \) completely splits in \( K \).

4.2.2. In diagrams, the normality of an extension is indicated by a double line: \( \frac{K}{F} \)

4.2.3. Every quadratic extension is normal.

4.2.4. **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.

4.2.5. **Theorem.** An algebraic extension \( K/F \) is normal iff for any extension \( E/K \), any embedding of \( K/F \) into \( E/F \) is an automorphism of \( K/F \).

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 \( \alpha \) over \( F \) are in \( K \). (That is, the minimal polynomial of \( \alpha \) over \( F \) splits in \( K \)). Then \( K/F \) is normal. In particular, the splitting field of any family \( F \subseteq F[x] \) is a normal extension of \( F \).

4.2.7. **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.

The extension \( E/F \) is called the **normal closure** of \( K/F \). It is finite if \( K/F \) is finite.

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

4.3. **Galois extensions**

4.3.1. A finite normal separable extension is called a **Galois extension**.
4.3.2. By Theorem 4.1.6 we have:

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

4.3.3. If \( K/F \) is a Galois extension, then the group \( \text{Aut}(K/F) \) is called the Galois group of \( K/F \), and is denoted by \( \text{Gal}(K/F) \). By Theorem 4.3.2, \( \text{Gal}(K/F) \) 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 \( G = \text{Gal}(K/F) \) of a Galois extension \( K/F \) is defined by its action on the generators of \( K/F \), which are mapped to some their conjugates. The action of \( G \) on every set of elements of \( K \) conjugate over \( F \) is transitive.

4.3.5. **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 \( F[x] \).

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

4.3.7. **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.

4.3.8. If \( K/F \) is a finite separable extension, then its normal closure is a Galois extension, 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 use this to prove the following theorems:

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.

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.

4.5. Examples of Galois groups

4.5.1. 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 \( \varphi_i \) on the elements \( \sqrt{2} \) and \( \sqrt{3} \), generating the splitting field of \( f \), is given by

\[
\varphi_1 : \sqrt{2} \rightarrow -\sqrt{2}, \quad \varphi_2 : \sqrt{2} \rightarrow \sqrt{2}, \quad \varphi_3 : \sqrt{3} \rightarrow -\sqrt{3}.
\]

4.5.2. Let \( \omega = e^{2\pi i/3} \) and \( \alpha = \sqrt{2} \). The Galois group \( G \) of the polynomial \( f(x) = x^3 - 2 \) over \( \mathbb{Q} \) acts as a group of all permutations of the roots \( \alpha, \omega\alpha, \omega^2\alpha \) of \( f \), and 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 \( \sqrt{2} \), generating the splitting field of \( f \), is given by

\[
\sigma : \omega \rightarrow \omega, \quad \tau_1 : \omega \rightarrow \omega^2, \quad \tau_2 : \omega \rightarrow \omega^2, \quad \tau_3 : \omega \rightarrow \omega^2 \alpha.
\]

4.5.3. Let \( F \) be a field with \( \text{char} F \neq 2 \) 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 \( \alpha = \frac{1}{\sqrt{2}}(-a + \sqrt{a^2 - 4b}) \) and \( \beta = \frac{1}{\sqrt{2}}(-a - \sqrt{a^2 - 4b}) \), with \( \alpha\beta = \sqrt{b} \). Let \( K \) be the splitting field of \( f \), \( K = F(\alpha, \beta) \). It is easy to see that automorphisms of \( K/F \) act
on the set of roots of $f$ so that the square

\[
\begin{array}{c|c}
\alpha & \beta \\
\hline
-\beta & -\alpha \\
\end{array}
\]

is preserved, and so, $G = \text{Gal}(f)$ is isomorphic to a subgroup of $D_8$. Namely, if $\sqrt{b} \in F$, then $G \cong V_4$; if $\sqrt{b} \notin F$ and $\sqrt{\alpha^2 - 4b}/\sqrt{b} \in F$, then $G \cong \mathbb{Z}_4$; and if both $\sqrt{b}, \sqrt{\alpha^2 - 4b}/\sqrt{b} \notin F$, then $G \cong D_8$.

**4.5.4.** Let $\omega$ be a primitive $n$th root of unity over $\mathbb{Q}$; say, $\omega = e^{2\pi i/n}$. The Galois group $G$ of the cyclotomic extension $\mathbb{Q}(\omega)/\mathbb{Q}$ is $G = \{ \phi_k : (k, n) = 1 \}$, where the action of $\phi_k$ for every $k$ is defined by $\phi_k(\omega) = \omega^k$. So, $G$ is isomorphic to the multiplicative group $\mathbb{Z}_n^*$.

**4.5.5.** Let $L$ be the $n$th 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 $L(\alpha)$ where $\alpha = \sqrt[4]{2}$. If $x^n - 2$ is irreducible over $L$, then the Galois group $G = \text{Gal}(f) = \text{Gal}(L(\alpha)/L)$ is cyclic, isomorphic to $\mathbb{Z}_n$, and generated by the automorphism $\varphi$ defined by $\varphi(\alpha) = \omega \alpha$.

**4.5.6.** The Galois group of the finite field $\mathbb{F}_{p^n}$, $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, is cyclic, isomorphic to $\mathbb{Z}_n$, and is generated by the Frobenius automorphism.

### 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 $\text{Gal}(K/L) \leq \text{Gal}(K/F)$. We therefore have a mapping $L \mapsto \text{Gal}(K/L)$ 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 and $H$ 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** $H$ if all elements of $S$ are fixed by $H$. By $\text{Fix}(H)$ 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 $H \leq \text{Aut}(K/F)$, then $\text{Fix}(H)$ is an extension of $F$. We therefore have a mapping $H \mapsto \text{Fix}(H)$ 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 $G = \text{Gal}(K/F)$. Then the mappings $L \mapsto \text{Gal}(K/L)$ and $H \mapsto \text{Fix}(H)$ 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 $F = \text{Fix}(G)$. Then $[K : F] = |G|$.

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

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

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

**4.6.6. The fundamental Galois theorem – full version.** Let $K/F$ be a Galois extension and let $G = \text{Gal}(K/F)$. 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 $L \mapsto \text{Gal}(K/L)$). Then


(ii) $L_1 \subseteq L_2$ if and only if $H_1 \supseteq H_2$, and in this case, $[L_2 : L_1] = [H_1 : H_2]$. 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 $K$ 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 $G$. 

12
(v) For any $\varphi \in G$, the subgroup of $G$ corresponding to $\varphi(L)$ 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 $\varphi \mapsto \varphi\vert_L$ defines a homomorphism $\text{Gal}(K/F) \to \text{Gal}(L/F)$ and induces an isomorphism $G/H \cong \text{Gal}(L/F)$.

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

4.7.1. The diagram of subextensions of the biquadratic extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ (see 4.5.1), along with the diagram of subgroups of its Galois group:

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 $\alpha = \sqrt[3]{2}$ (see 4.5.2), with the diagram of subgroups of its Galois group:

4.7.3. The diagram of subfields of a finite field $\mathbb{F}_{p^n}$ is the same as the diagram of subgroups of the cyclic group $\mathbb{Z}_n$.

5. Composites and towers of Galois extensions

5.1. 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 $\text{Gal}(KL/FL)$ is (isomorphic to) a subgroup of $\text{Gal}(K/F)$.

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 $\text{Gal}(K/F) \cong \text{Gal}(K/L_1) \rtimes \text{Gal}(L_1/F)$, $\text{Gal}(K/L_2) \cong \text{Gal}(L_1/F)$, and $[K : F] = [L_1 : F] \cdot [L_2 : F]$.

5.2.2. Example. Let $K$ be the splitting field of the polynomial $x^n - 2 \in \mathbb{Q}[x]$ for some $n \in \mathbb{N}$. Then $K = \mathbb{Q}(\omega, \alpha)$ where $\omega$ is a primitive $n$th root of unity and $\alpha = \sqrt[3]{2}$. 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 $\text{Gal}(L_1/\mathbb{Q}) \cong \mathbb{Z}_n^\ast$ and $\text{Gal}(K/L_1) \cong \mathbb{Z}_n$. 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 $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_n$. 

13
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 \( \text{Gal}(K/F) \cong \text{Gal}(K/L_1) \times \text{Gal}(L_1/F) \), \( \text{Gal}(K/L_2) \cong \text{Gal}(L_1/F) \), \( \text{Gal}(K/L_1) \cong \text{Gal}(L_2/F) \), and \( [K:F] = [L_1:F] \cdot [L_2:F] \):

\[
\begin{array}{c|c}
L_1 \cap L_2 = K & \text{m} \\
\hline
H_1 \cap H_2 = 1 & \text{m} \\
H_1 / H_2 & L_1 \times L_2 \\
H_1 \times H_2 & L_1 \times L_2 \\
\end{array}
\]

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, \( \text{Gal}(K/F) \cong \text{Gal}(L_1/F) \times \text{Gal}(L_2/F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \).

(ii) 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 \( L_2 \) is the splitting field of \( x^3 - 3 = \mathbb{Q}(e^{2\pi i/3}, \sqrt{3}) = \mathbb{Q}(\sqrt{3}, \sqrt{3}) \). Both \( L_1 \) and \( L_2 \) are normal extensions of \( \mathbb{Q} \), and \( L_1 \cap L_2 = \mathbb{Q} \), so \( \text{Gal}(K/F) \cong \text{Gal}(L_1/F) \times \text{Gal}(L_2/F) \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \).

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 \( G = \text{Gal}(K/F) \), \( H_1 = \text{Gal}(K/L_1) \) and \( H_2 = \text{Gal}(K/L_2) \). By Theorem 5.3.1 we have the diagrams

\[
\begin{array}{c|c}
H_1 \cap H_2 = 1 & L_1 \cap L_2 = 1 \\
\hline
H_1 \times H_2 & L_1 \times L_2 \\
H_1, H_2 & L_1, L_2 \\
\end{array}
\]

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 \( N_1 = \text{Gal}(L_1/F) \) and \( N_2 = \text{Gal}(L_2/F) \). Then \( N_1 \cong \mathbb{G}/H_1 \), 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 \( \eta: G \rightarrow N_1 \times N_2 \), \( \varphi \mapsto (\varphi|_{L_1}, \varphi|_{L_2}) \), which is injective since \( L_1L_2 = K \). \( \eta \) is not, however, surjective: if \( \varphi_1 \in \varphi|_{L_1} \) and \( \varphi_2 \in \varphi|_{L_2} \), then \( \varphi_1|_{L_1 \cap L_2} = \varphi_2|_{L_1 \cap L_2} \). Let \( D = \text{Gal}((L_1 \cap L_2)/F) \), then \( D = G/(H_1H_2) \cong N_1/(H_1H_2)/H_2 \cong N_2/(H_1H_2) \) is a common factor of \( N_1 \) and \( N_2 \); let \( \tau_1: N_1 \rightarrow D \) and \( \tau_2: N_2 \rightarrow D \) be the factorization mappings. Then the image of \( \eta \) lies in the subgroup

\[
N_1 \times_D N_2 = \{ (\varphi_1, \varphi_2) : \tau_1(\varphi_1) = \tau_2(\varphi_2) \}
\]

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 \( f(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x] \). Then \( K = L_1L_2 \), where \( L_1 \) and \( L_2 \) are the splitting fields of \( x^2 - 2 \) and of \( x^2 - 3 \) respectively, \( L_1 = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) and \( L_2 = \mathbb{Q}(\sqrt{6}, \sqrt{6}) \). Both \( L_1 \) and \( L_2 \) are normal extensions of \( \mathbb{Q} \), \( L_1 \cap L_2 = \mathbb{Q}(\sqrt{6}) \), so \( \text{Gal}(K/F) \cong \text{Gal}(L_1/F) \times \text{Gal}(L_2/F) \cong \mathbb{S}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \).

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 \( L_1 \otimes_F \cdots \otimes_F L_n \rightarrow K \) 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 \( L_i \cap \{ L_1 \cdots L_{i-1}L_{i+1} \cdots L_n \} = F \).

5.4.2. Let \( K/F \) be a Galois extension whose Galois group \( G = \text{Gal}(K/F) \) is a direct product, \( G = H_1 \times \cdots \times H_k \), of subgroups \( H_1, \ldots, H_k \). Then each of \( H_i \) is normal in \( G \). For each \( H_i \) 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 \( L_i = \text{Fix}(N_i) \); then \( L_i/F \) are Galois extensions with \( \text{Gal}(L_i/F) \cong G/N_i \cong H_i \). We have \( L_1 \cdots L_n = K \) and \( \prod_{i=1}^n |H_i:F| = \prod_{i=1}^n |H_i| = |G| \), 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 \( \text{Gal}(L_i/F) = H_i, \ i = 1, \ldots, n \), such that for each \( i \), \( L_i \cap \{ L_1 \cdots L_{i-1} L_{i+1} \cdots L_n \} = F \), then by 5.3.1, \( K/F \) is Galois with \( \text{Gal}(K/F) \cong H_1 \times \cdots \times H_n \), and is a free composite of \( L_1/F, \ldots, L_n/F \).

5.5. Composites and the Galois closure 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 \( H_i = \text{Gal}(K/L_i) \); 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 \( i \), \( H_{i-1}/H_i \cong \text{Gal}(L_i/L_{i-1}) \).

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 \( i \), \( L_i = \text{Fix}(H_i) \), and \( \text{Gal}(L_i/L_{i-1}) \cong H_{i-1}/H_i \).

5.5.2. Let \( K = L_n/L_{n-1}/\cdots/L_1/L_0 = F \) and \( K' = L'_n/L'_{n-1}/\cdots/L'_1/L'_0 = F \) 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 subsection 5.1.1, for each \( j \), the group \( \text{Gal}((L_nL'_j)/(L_nL'_{j-1})) \) is isomorphic to a subgroup of \( \text{Gal}(L'_j/L_{j-1}) \). We obtain:

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

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 \( \text{Gal}(E/F) = \{ \varphi_1, \ldots, \varphi_n \} \). \( E \) 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

\[
\begin{array}{ccc}
\varphi_i: & K_i \rightarrow K & \\
\downarrow & & \downarrow \\
L & \rightarrow & L \\
\end{array}
\]

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

5.5.4. **Example.** Let \( \alpha = \sqrt{2} \), so that \( \alpha^2 = 2 \). Let \( K = K_1 = \mathbb{Q}(\alpha) \) and \( L = \mathbb{Q}(\alpha^2) \). The extensions \( K/L \) and \( L/Q \) are quadratic and so Galois, but the extension \( K/Q \) is not. The conjugates of \( \alpha \) over \( Q \) are \( \pm\alpha, \pm i\alpha \) (where \( i = \sqrt{-1} \)), and the Galois closure of \( K/Q \) is \( Q(\alpha, i\alpha) = K_1K_2 \) 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 \( \varphi \) that produces the commutative diagram

\[
\begin{array}{ccc}
\varphi: & K \rightarrow K_2 & \\
\downarrow & & \downarrow \\
L & \rightarrow & L \\
\end{array}
\]

is defined by \( \varphi(\alpha) = i\alpha \), and maps \( \alpha^2 \) 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 \( G = \text{Gal}(E/F) \). Then \( E/F \) is the composite of the extensions \( \varphi(K)/F, \varphi \in G \), and for each \( \varphi \), 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 \( \text{Gal}(\varphi(L_i)/\varphi(L_{i-1})) \cong \text{Gal}(L_i/L_{i-1}) \) for all \( i \). By Theorem 5.5.2, we obtain:
Theorem. If $K/F$ is a tower of Galois extensions, with Galois groups $N_1, \ldots, N_r$, then the Galois closure $E/F$ of $K/F$ is also a tower of Galois extensions, whose Galois groups are subgroups of $N_1, \ldots, N_r$. It follows that $\text{Gal}(E/F)$ has a subnormal series with factors being subgroups of $N_1, \ldots, N_r$.

6. Some applications of the Galois theory

6.1. More methods of finding the minimal polynomial of an algebraic element

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

6.1.2. Let $K/F$ be a separable extension, let $\alpha \in K$, let $L/F$ be a Galois subextension of $K/F$, and let $p = m_{\alpha,L}$, the minimal polynomial of $\alpha$ over $L$. Then $m_{\alpha,F}^k = \prod_{\varphi \in \text{Gal}(L/F)} \varphi(p)$, where $k = [L(\alpha) : F(\alpha)]$.

6.2. The norm of an algebraic element

6.2.1. Let $K/F$ be a finite separable extension, let $[K : F] = n$. Let $E/F$ be a Galois extension containing $K$, let $G = \text{Gal}(E/F)$ and $H = \text{Gal}(E/K)$. For $\alpha \in K$, the norm of $\alpha$ in $K$ is $N_{K/F}(\alpha) = \prod_{\varphi \in G/H} \varphi(\alpha)$. (Where $G/H$ is the set of left cosets of $H$ in $G$; it is not a group if $H$ is not normal in $G$.)

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 $m_{\alpha,F}(x) = x^n + \cdots + a_1x + a_0$; 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 $\alpha$, $T(x) = \alpha x$. Then $N_{K/F}(\alpha) = \det T$.

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. In particular, for every $\alpha \in K$, $F(\alpha)$ contains all conjugates of $\alpha$.

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 $L_i/F$ are Galois, with $\text{Gal}(L_i/F) \cong H_i$, and $L_i \cap (L_1 \cdots L_{i-1}L_{i+1} \cdots L_k) = F$, $i = 1, \ldots, k$.

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 $x^n - a$ over $\mathbb{Q}$

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 ones of the form $F(\sqrt[n]{a})/F$ with $d \mid n$. In particular, the only nontrivial normal subextension of $F(\sqrt[n]{a})/F$, and only if $n$ is even, is $F(\sqrt[n]{a})/F$.

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 $\sqrt[n]{a} \in N$, is a quadratic extension. If $F = \mathbb{Q}$, by 5.2.1, in the first case $[KN : F] = n\varphi(n)$ and $\text{Gal}(x^n - a) = \text{Gal}(KN/F) \cong \mathbb{Z}_n \rtimes \mathbb{Z}_n^n$, and in the second case, by 5.2.1 applied to $K$ and $N$ as extensions of $K \cap N$, $[KN : F] = n\varphi(n)/2$, and $\text{Gal}(x^n - a)$ is a “relative semidirect product” $\mathbb{Z}_n \rtimes_{\varphi} \mathbb{Z}_n^n$. 

16
6.5. The theorem on a primitive element

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

6.5.2. Proposition. A finite separable extension may only have finitely many subextensions.

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

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 \( \text{Gal}(K/F) \) is a subgroup of \( S_n \).

6.5.5. Theorem 6.5.3 does not hold for inseparable extensions: take \( K = F_p((x,y)) \) (the field of rational functions in two variables over \( F_p \)) and \( F = F_p(x^p,y^p) \); then \( [K:F] = p^2 \), but for every element \( h \in K \), \( h^p \in F \), so \( [F(h):F] \leq p \).

6.6. \( p \)-extensions

Let \( p \) be a prime integer.

6.6.1. Let us say that a finite extension is a \( p \)-extension if it is contained in a Galois extension of degree \( p^n \) for some \( n \in \mathbb{N} \) (and so, the Galois group of this Galois extension 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 Galois extensions of degree \( p \).

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

6.7. The fundamental theorem of algebra

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

6.8. Constructions with ruler and compass

6.8.1. Given a set \( S \) of points on the plane, of cardinality \( \geq 2 \), 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 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.

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 \( \mathbb{Q} \).

6.8.3. 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 \( F \).

6.8.4. A complex number \( a+bi \) is said to be constructible over a real field \( F \) iff both \( a \) and \( b \) are constructible over \( F \).

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

6.8.5. From 6.6.5 we obtain:
Theorem. A complex number $\alpha$ is constructible over a real field $F$ iff the splitting field of $\alpha$ over $F$ is a $2$-extension.

6.8.6. The following problems are non-solvable with ruler and compass:

(i) Squaring a circle: Construct a square having the area of the unit circle; or, in coordinates: construct an $a \in \mathbb{R}$ such that $a^2 = \pi$.

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

(iii) Trisecting an angle: Given an angle $\theta$, construct the angle $\theta/3$; or, in coordinates: given $b \in \mathbb{R}$ (that is assumed to be the cosine of $\theta$) construct $a \in \mathbb{R}$ (the cosine of $\theta/3$) such that $b = 4a^3 - 3a$.

6.8.7. Proposition. A regular $n$-gon is constructible iff $\varphi(n)$ is a power of $2$ (where $\varphi$ is Euler’s function).

6.8.8. Proposition. A regular $n$-gon is constructible iff $n = 2^r p_1 \cdots p_t$ where $p_i$ are distinct Fermat’s primes (primes of the form $2^{2^k} + 1$ with integer $s > 0$).

6.9. Linear independence of square roots of square free integers

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

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

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

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

6.10. The theory of symmetric rational functions

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

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

6.10.3. If a monic polynomial $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$, of degree $n$, has roots $\alpha_1, \ldots , \alpha_n$, then, up to the sign, the coefficients of $f$ are just the elementary symmetric polynomials of $\alpha_i$: $a_1 = -s_1(\alpha_1, \ldots , \alpha_n)$, $a_2 = s_2(\alpha_1, \ldots , \alpha_n)$, ..., $a_n = (-1)^ns_n(\alpha_1, \ldots , \alpha_n)$.

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 $h \in R[x_1, \ldots , x_n]$ there exists a unique $g \in R[y_1, \ldots , y_n]$ such that $h(x_1, \ldots , x_n) = g(s_1, \ldots , s_n)$.

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:

**Theorem.** For any field $F$ and $n \in \mathbb{N}$, every symmetric rational function $h \in F(x_1, \ldots , x_n)$ is representable in the form $h(x_1, \ldots , x_n) = g(s_1, \ldots , s_n)$ with $g \in F(y_1, \ldots , y_n)$.

6.10.6. We also obtain that for any field $F$ and $n \in \mathbb{N}$, the general polynomial $G(x) = x^n - s_1x^{n-1} + \cdots + (-1)^ns_n \in L[x]$, where $L = F(s_1, \ldots , s_n)$, the field of symmetric rational functions, has $\text{Gal}(G/L) \cong S_n$.

6.10.7. Here is another corollary of Theorem 6.10.5:

**Theorem.** Let $F$ be a field, let $f(x) = x^n + a_1x^{n-1} + \cdots + a_n \in F[x]$, and let $\alpha_1, \ldots , \alpha_n$ be the roots of $f$ (in the splitting field of $f$). Then for any symmetric polynomial $h$ in $n$ variables, $h(\alpha_1, \ldots , \alpha_n) \in F$. 

18
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 \( \alpha \) of an extension of \( F \) such that \( \alpha^n = a \). An extension \( K/F \) is said to be radical (or simple radical) if \( K = F(\sqrt[n]{\alpha}) \) 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.

7.1.4. An element \( \alpha \), algebraic over \( F \), is said to be expressible by radicals (or can be solved for in terms of radicals) over \( F \) if \( \alpha \) 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.

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 \( K/L \) is cyclic. If, additionally, \( L/F \) is normal, then it is also cyclic.

7.2.3. An extension is said to be polycyclic if it is a tower of cyclic extension.

7.2.4. Theorem. (i) Any tower of polycyclic extensions is polycyclic.

(ii) Any composite of polycyclic extensions is polycyclic.

(iii) The Galois closure of a polycyclic extension is 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 polycyclic iff it is solvable.

7.2.6. Theorem. A Galois extension is polycyclic iff it is solvable.

7.3. Radical and cyclic extensions

7.3.1. Theorem. Let \( n \in \mathbb{N} \), let \( F \) be a field of characteristic not dividing \( n \) that contains \( n \)th roots of unity, and let \( a \in F \). Then \( K = F(\sqrt[n]{a}) \) is a cyclic extension of \( F \) of degree dividing \( n \).

7.3.2. Let \( n \in \mathbb{N} \), and let \( F \) be a field of characteristic not dividing \( n \) that contains a primitive \( n \)th root of unity \( \omega \). Let \( K/F \) be a cyclic extension of degree \( n \), and let \( \varphi \) be a generator of \( \text{Gal}(K/F) \). For \( \alpha \in K \), the Lagrange resolvent \((\alpha, \omega)\) 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 \( \alpha \in K \), \( \varphi((\alpha, \omega)) = \omega^{-1}(\alpha, \omega) \), and \( \varphi((\alpha, \omega)^n) = (\alpha, \omega)^n \), so \((\alpha, \omega)^n \in F\).

7.3.4. Theorem. Let \( n \in \mathbb{N} \), let \( F \) be a field of characteristic not dividing \( n \) that contains \( n \)th roots of unity, 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 \( a \in F \). \( \alpha \) is \((\alpha, \omega)^n \) for some \( \alpha \in K \).

7.4. Solvability of polynomials in radicals

In what follows, we will assume that the basic field \( F \) has characteristic which doesn’t divide the degree of all extensions involved (zero characteristic is preferable).

7.4.1. Theorem. If \( K/F \) is an extension of degree \( n \) and \( F \) contains a primitive \( n \)th root of unity, then \( K/F \) is polyradical iff it is polycyclic.

7.4.2. Theorem. An element \( \alpha \) is expressible by radicals over \( F \) iff \( \alpha \) is contained in a solvable extension of \( F \). In this case, all conjugates of \( \alpha \) are also expressible by radicals over \( F \).
Applying the Galois theory to cyclotomic extensions, we can express by radicals the roots of unity themselves.  

7.4.6. 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 $\sqrt[3]{1} = -\frac{1}{2} + \frac{\sqrt{3}}{2}$, $\sqrt[5]{1} = \frac{1}{2} \pm i \frac{\sqrt{3}}{2}$, $\sqrt[3]{2} = -\frac{1}{2} + \frac{\sqrt{3}}{2}$, and $\sqrt[5]{2} = \frac{1}{2} \pm i \frac{\sqrt{3}}{2}$. (However, at least theoretically, I don’t see why these are better than “the radical” $\sqrt[3]{2}$.)

### 7.4.3. Theorem
A polynomial $f \in F[x]$ is solvable in radicals iff the group $\text{Gal}(f)$ is solvable. If $f$ is irreducible and one of its roots is expressible by radicals, then $f$ is solvable in radicals.

### 7.4.4. Corollary
Every polynomial $f \in F[x]$ of degree $\leq 4$ is solvable in radicals. The general polynomial of degree $\geq 5$ (see 6.10.5) is not solvable in radicals.

### 7.4.5. 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.

**Example.** $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ is unsolvable in radicals.

7.4.6. 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 $\sqrt[3]{1} = -\frac{1}{2} + \frac{\sqrt{3}}{2}$, $\sqrt[5]{1} = \frac{1}{2} \pm i \frac{\sqrt{3}}{2}$, $\sqrt[3]{2} = -\frac{1}{2} + \frac{\sqrt{3}}{2}$, and $\sqrt[5]{2} = \frac{1}{2} \pm i \frac{\sqrt{3}}{2}$. (However, at least theoretically, I don’t see why these are better than “the radical” $\sqrt[3]{2}$.)

### 7.5. The alternating group and the discriminant of a polynomial
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 $\text{Gal}(f)$, 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 $\text{Disc}(f)$ or $D(f)$. Notice that $D(f) = 0$ iff $f$ has a multiple root.

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

(ii) For a cubic polynomial $f(x) = x^3 + ax^2 + bx + c$, $D(f) = a^3b^2 + 18abc - 4b^3 - 4a^3c - 27c^2$, and for $f(x) = x^3 + px + q$, $D(f) = -4p^3 - 27q^2$.

(iii) For a quartic polynomial $f(x) = x^4 + px^2 + qx + r$, $D(f) = -27p^4 - 108pq^2 - 162p^2q^2 - 27r^2 - 256r^3$.

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

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 $\sqrt[n]{D(f)} \in F$, then $\text{Gal}(f)$ is trivial, and $f$ splits in $F$, otherwise $\text{Gal}(f) \cong \mathbb{Z}_2$ and the splitting field of $f$ is $F(\sqrt[n]{D(f)})$. (And indeed, the roots of $f$ are $\frac{1}{2}(-a \pm \sqrt[n]{D(f)})$.)

### 7.6. The Galois groups 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 $G = \text{Gal}(f)$, 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 $G \cong A_3 \cong \mathbb{Z}_3$. By Theorem 7.5.3, if $\sqrt[n]{D(f)} \in F$, then $G \cong \mathbb{Z}_3$, and otherwise $G \cong S_3$.

7.7. For $f \in \mathbb{Q}[x]$, $f$ has one real and two complex (non-real) roots iff $D < 0$, in which case $G \cong S_3$; $f$ has all three roots real iff $D > 0$ (in which case $G \cong S_3$ or $\mathbb{Z}_3$).

7.7.1. Adjoin to $F$ a primitive 3rd root of unity $\omega = \omega^3 = \frac{-1 + \sqrt{3}}{2}$, that is, put $\tilde{F} = F(\sqrt{3})$, and let $\tilde{K} = K(\sqrt{3})$. Since $\tilde{K}$ is a cyclic cubic extension of $\tilde{F}(\sqrt{3})$, it is radical, $\tilde{K} = \tilde{F}(\sqrt[3]{\gamma})$ for some $\gamma$ with $\gamma^3 \in \tilde{F}(\sqrt{3})$. The element $\gamma$ can be found as the Lagrange resolvent of an element of $\tilde{K}$, say, of a root of $f$; for $f(x) = x^3 + px + q$, computations give

$$
\gamma = -\frac{27}{2}q + \frac{3}{2}\sqrt{-3D} \quad \text{and} \quad \gamma' = -\frac{27}{2}p - \frac{3}{2}\sqrt{-3D},
$$

20
and the roots of $f$ are

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

These formulas for roots of a cubic are called Cardano’s formulas.

7.7.2. *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.

7.8. The Galois groups 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 $G = \text{Gal}(f)$, and let $D = D(f)$.

7.8.1. After replacing $x + a_3/4$ by $x$, $f$ takes the form $f(x) = x^3 + px^2 + qx + r$; this operation changes neither $K$, nor $G$, nor $D$.

7.8.2. $G$ 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 $H_1 = \langle (1, 3, 2, 4), (1, 2) \rangle$, $H_2 = \langle (1, 2, 3, 4), (1, 3) \rangle$, $H_3 = \langle (1, 2, 4, 3), (1, 4) \rangle$ of order 8, isomorphic to $D_8$;
(iv) the normal subgroup $V = \langle (1, 2, 3)(4), (1, 3)(2, 4), (1, 4)(2, 3) \rangle$, of order 4, isomorphic to the Klein 4-group $V_4 \cong \mathbb{Z}_2^2$;
(v) and three conjugate cyclic subgroups $C_1 = \langle (1, 3, 2, 4) \rangle$, $C_2 = \langle (1, 2, 3, 4) \rangle$, $C_3 = \langle (1, 2, 4, 3) \rangle$, of order 4, isomorphic to $\mathbb{Z}_4$.

7.8.3. The group $S_4$ is solvable and has the normal series $1 \triangleleft V \triangleleft A_4 \triangleleft S_4$, 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 $1 \triangleleft (V \cap G) \triangleleft (A_4 \cap G) \triangleleft G$, and the corresponding tower for $K$ is $K/L/F(\sqrt{D})/F$ where $L = \text{Fix}(V \cap G)$:

```
        1        4 or 2 or 1
V \cap G      \quad L
        3 or 1
A_4 \cap G  \quad F(\sqrt{D})
        2 or 1
        G      \quad F
```

7.8.4. 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 $\theta_1, \theta_2$ and $\theta_3$, 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 $f$.

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

7.8.5. **Theorem.** Let us interpret $G$ as a subgroup of $S_4$ and use notation from 7.8.2. 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 $G = V$. 

21
(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 $C_1$ (and is isomorphic to $\mathbb{Z}_4$).

7.8.6. The roots $\theta_i$ of the cubic resolvent $R$ of $f$ are expressible in radicals with the help of Cardano’s formulas, and then, for $f(x) = x^4 + px^2 + qx + r$,

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

7.9. Computation of Galois groups

7.10. The following effective algorithm for computing Galois groups of polynomials belongs to van der Waerden: Let $f \in F[x]$ be an irreducible separable polynomial of degree $n$, let $\alpha_1, \ldots, \alpha_n$ be the roots of $f$, let $K = F(\alpha_1, \ldots, \alpha_n)$. Let $x_1, \ldots, x_n$ be variables; for each $\sigma \in S_n$ let $\theta_\sigma = \alpha_{\sigma(1)}x_1 + \cdots + \alpha_{\sigma(n)}x_n$, and let $g(x) = \prod_{\sigma \in S_n}(x - \theta_\sigma)$. Then $g$ is $S_n$-invariant, its coefficients are symmetric functions of $\alpha_1, \ldots, \alpha_n$, so $g \in F[x_1, \ldots, x_n][x]$. Let $g = g_1 \cdots g_k$ be the factorization of $g$ into irreducible polynomials over $F(x_1, \ldots, x_n)$. Elements of $S_n$ permute the polynomials $g_i$; let $G$ be the stabilizer of $g_1$. Then $G = \text{Gal}(f/F)$.

7.10.1. 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 $f = f \mod p \in \mathbb{F}_p[x]$. We don’t prove the following theorem:

**Theorem.** As groups of permutations of the roots of $f$ and the corresponding roots of $\tilde{f}$, $\text{Gal}(\tilde{f}/\mathbb{F}_p)$ is a subgroup of $\text{Gal}(f/\mathbb{Q})$.

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

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

7.11. As a corollary, we obtain that for every $n \in \mathbb{N}$ there exists a polynomial $f \in \mathbb{Q}[x]$ such that $\text{Gal}(f/\mathbb{Q}) \cong S_n$.

8. Introduction to the theory of transcendental extensions

The theory of transcendental extensions reminds 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 $\alpha_1, \ldots, \alpha_k \in A$ there is a nonzero polynomial $f \in F[x_1, \ldots, x_k]$ such that $f(\alpha_1, \ldots, \alpha_k) = 0$; $A$ is said to be **algebraically independent** otherwise.

**8.0.2.** Let $K/F$ be an extension; a maximal algebraically independent over $F$ subset $B$ of $K$ is called a **transcendence base of $K/F$**.

**8.0.3.** $B$ is a transcendence base of $K/F$ iff $K/F(B)$ is an algebraic extension.

**8.0.4. Theorem.** For any extension $K/F$, a transcendence base of $K/F$ exists. All transcendence bases of $K/F$ have the same cardinality.

The cardinality of a transcendence base of $K/F$ is called the **transcendence degree of $K/F$**.

**8.0.5.** 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 $x_\alpha, \alpha \in B$.

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