Lecture Notes
in
Galois Theory

Gunnar Traustason
(2nd semester 2017)
1 The polynomial ring $\mathbb{K}[x]$

I. Some general recap on rings

**Definition.** A *ring* is a set equipped with two binary operations $+$ (addition) and $\cdot$ (multiplication) such that

a) $R$ is an abelian group under addition:

1) $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$
2) $a + b = b + a$ for all $a, b \in R$
3) There exists $0 \in R$ such that $a + 0 = a$ for all $a \in R$
4) For all $a \in R$ there exists an element $-a \in R$ such that $a + (-a) = 0$.

b) $R$ is associative with 1 under multiplication:

5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$
6) There exists $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$.

c) $R$ satisfies the distributive laws:

7) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$
8) $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in R$.

**Remarks.** 1) Recall that 0, 1 are unique, called the additive and multiplicative identities.
2) Recall that $a \cdot 0 = 0 \cdot a = 0$ and $a(-b) = (-a)b = -ab$.

**Definition.** A ring $R$ is said to be *commutative* if $ab = ba$ for all $a, b \in R$.

**Definition** A subset $S$ of a ring $R$ is said to be a *subring*, if $1_R \in S$ and $a + b, ab, -a \in S$ whenever $a, b \in S$. We use the notation $S \leq R$ for ‘$S$ is a subring of $R$’.

**Remark.** Notice that if $S \leq R$, then $0_R = 1_R + (-1_R) \in S$.

**Definition.** 1) A nonempty subset of a commutative ring $R$ is an *ideal* if $-a, a + b, ra \in I$ whenever $a, b \in I$ and $r \in R$. We then sometimes write $I \trianglelefteq R$ for ‘$I$ is an ideal of $R$’.

2) An ideal $I$ of a commutative ring is a principal ideal if $I = Ra$ for some $a \in R$. 

**Definition.** Let \( R \) be a commutative ring.

1) \( R \) is an **integral domain** (ID) if \( R \neq \{0\} \) and satisfies

\[
ab = 0 \Rightarrow a = 0 \text{ or } b = 0.
\]

2) \( R \) is a **principal ideal domain** (PID) if \( R \) is an integral domain and every ideal of \( R \) is a principal ideal.

**Quotient rings.** Let \( R \) be a commutative ring with an ideal \( I \). The **quotient ring** \( R/I \) is

\[
R/I = \{\bar{a} = a + I : a \in R\}
\]

where the addition and multiplication are given by

\[
(a + I) + (b + I) = a + b + I, \quad (a + I)(b + I) = ab + I.
\]

\( R/I \) then becomes a ring with \( \bar{0} = 0 + I \) and \( \bar{1} = 1 + I \) as the additive and multiplicative identities. The additive inverse of \( a + I \) is \( -a + I \).

**The characteristic of a ring.** The characteristic, \( \text{char } R \), of \( R \) is a non-negative integer defined as follows:

If there exists a positive integer \( n \) such that

\[
n1_R = 1_R + \cdots + 1_R = 0_R,
\]

then \( \text{char } R \) is the smallest such positive integer. If no such positive integer exists then \( \text{char } R = 0 \).

**Remarks.** (1) If \( \text{char } R = 1 \) then \( 1_R = 0_R \) and \( a = 1_R \cdot a = 0_R \cdot a = 0_R \) for all \( a \in R \). Thus \( R = \{0\} \) is the only ring with characteristic 1.

(2) If \( \text{char } R = n > 0 \) then \( na = n1_R \cdot a = 0_R \cdot a = 0_R \) for all \( a \in R \). That is \( nR = 0 \).

**Example.** \( \text{char } \mathbb{Q} = 0 \) and the characteristic of \( \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \) is \( n \).

**Definition.** Let \( R, S \) be rings. A map \( \phi : R \to S \) is said to be a **ring homomorphism** if:

\[
\phi(a + b) = \phi(a) + \phi(b)
\]

\[
\phi(ab) = \phi(a) \cdot \phi(b)
\]

\[
\phi(1_R) = 1_S
\]

If \( \phi \) is bijective, then we say that \( \phi \) is a **ring isomorphism**. We often write \( R \cong S \) for ‘\( R \) isomorphic to \( S \)’.

**Remarks.** Recall that \( \phi(0_R) = 0_S \) and \( \phi(-a) = -\phi(a) \).

**First ring isomorphism theorem.** If \( \phi : R \to S \) is a ring homomorphism the \( \text{im } \phi \leq S \), \( \ker \phi \triangleleft R \) and

\[
\text{im } \phi \cong R/\ker \phi.
\]
Here \( \text{im}\, \phi = \{ \phi(a) : a \in R \} \) and \( \ker \phi = \{ a \in R : \phi(a) = 0 \} \).

**Remark.** Recall that \( \phi \) is injective if and only if \( \ker \phi = \{0\} \).

### The smallest subring of \( R \)

A subring \( S \) of a given ring \( R \) contains \( 1_R \) and thus \( \mathbb{Z}1_R = \{ n1_R : n \in \mathbb{Z} \} \). Notice that we have a ring homomorphism

\[
\phi : \mathbb{Z} \to R, \, n \mapsto n1_R.
\]

In particular \( \mathbb{Z}1_R = \text{im}\, \phi \) is a subring of \( R \) and clearly the smallest subring. There are two possible scenarios.

If \( \text{char} \, R = n > 0 \) then \( \ker \phi = n\mathbb{Z} \) and by the first isomorphism theorem we have \( \mathbb{Z}1_R = \text{im}\, \phi \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n \).

If \( \text{char} \, R = 0 \) then \( \ker \phi = \{0\} \) and \( \phi \) is injective. Hence in this case \( \mathbb{Z}1_R = \text{im}\, \phi \cong \mathbb{Z} \).

### II. Some basic facts about fields

**Definition.** A commutative ring \( R \neq \{0\} \) is a **field** if for every \( 0 \neq a \in R \) there is \( b \in R \) such that \( ab = 1 \).

**Remarks.** (1) The element \( b \) is unique and is called the multiplicative inverse of \( a \). It is normally denoted \( a^{-1} \) or \( 1/a \).

(2) One could also say that a commutative ring \( R \neq \{0\} \) is a field if \( R \setminus \{0\} \) is a group.

(3) Every field is an ID. If \( ab = 0 \) and \( a \neq 0 \) then \( b = a^{-1}(ab) = a^{-1} \cdot 0 = 0 \).

**Definition.** A subset \( K \) of a field \( F \) is a subfield if it is a subring that is furthermore closed under taking inverses of non-zero elements. Thus \( K \) is a subfield if \( 1_F \in K \) and \( a + b, ab, -a \in K \) whenever \( a, b \in K \) and if furthermore \( a^{-1} \in K \) whenever \( 0 \neq a \in K \).

**Remark.** In fact \( K \) is a subfield of \( F \) if and only if \( K \) is a field in its own right with respect to the induced addition and multiplication from \( F \).

**Remark.** Notice that in the last remark, we do not have to include the requirement that \( 1_F \in K \). The reason for this is that we are already assuming that \( K \) is a field and from

\[
1_K \cdot 1_F = 1_K = 1_K \cdot 1_K,
\]

cancellation by \( 1_K \neq 0 \) gives \( 1_F = 1_K \in K \). However without the assumption that \( K \) is already a field this argument doesn’t work. For example \( \{0_F\} \) is not a subfield of \( F \). Hence the requirement \( 1_F \in K \) is needed in our definition of a subfield above.

**Proposition 1.1** If \( R \) is an integral domain then \( \text{char} \, R \) is either 0 or a prime number.

**Proof** As \( R \neq \{0\} \) we have that \( \text{char} \, R \neq 1 \). We argue by contradiction and suppose that \( \text{char} \, R = rs \) where \( 1 < r, s < \text{char} \, R \). But then

\[
rs1_R = 0_R
\]
whereas $r1_R, s1_R$ are non-zero. This contradicts the fact that $R$ is an ID. □

**Remark.** As every field is an ID the last proposition holds in particular for fields.

**Definition.** Let $K$ be a field. The *prime subfield* of $K$ is the intersection of all the subfields of $K$.

**Remark.** It is not difficult to see that the intersection of all the subfields is a subfield as well. Thus the prime subfield of $K$ is the unique smallest subfield of $K$.

From last proposition and the discussion at the end of Section I, we thus know that if $K$ is a field, whose characteristic is a prime number $p$, then its smallest subring $Z1_K$ is isomorphic to $Z_p$ that is a field and thus the prime subfield of $K$.

We are thus only left with the situation when char $K = 0$. In this case we have seen that the smallest subring $Z1_K$ of $K$ is isomorphic to $Z$ that is not a field. Here the prime subfield is

$$\left\{ \frac{n1_K}{m1_K} : n, m \in Z \text{ where } m \neq 0 \right\}$$

that is isomorphic to the field $Q$. Thus every field of characteristic 0 contains a copy of $Q$ as a subfield. (See exercise sheet 1 for the details).

**Definition.** We say that a field $K$ is a *prime field* if it has no proper subfields.

**Remark.** From the discussion above we see that up to isomorphisms the prime fields are $Q$ and $Z_p$, $p$ a prime number.

### III. Factorization in the polynomial ring $K[x]$  

Let $K$ be any field and consider the ring $K[x]$ of all polynomials

$$f = a_0 + a_1x + \cdots + a_n x^n$$

over $K$ where $n \geq 0$ and $a_0, \ldots, a_n \in K$.

**Definition.** If $f$ is a non-zero polynomial then the degree of $f$, $\deg f$, is the largest non-negative integer $m$ such that $a_m \neq 0$. If $f = 0$ then $\deg f = -\infty$.

**Remark.** Recall that $\deg fg = \deg f + \deg g$.

More generally we can consider polynomial rings over any commutative ring. Let $R$ and $S$ be commutative rings and suppose we have a homomorphism $\phi : R \to S$. We can use this homomorphism to extend it to an induced homomorphism $\phi^* : R[x] \to S[x]$.

Where

$$\phi^*(a_0 + a_1x + \cdots + a_n x^n) = \phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n.$$  

(See exercise sheet 1 for the details).
**Definition.** Let $R$ be an integral domain and let $f, g \in R$. We say that $f$ divides $g$ in $R$, and write $f | g$, if there exists $h \in R$ such that $g = fh$. We then also say that $f$ is a factor of $g$ in $R$.

**Remark.** Notice that $f | g$ in $R$ if and only if $Rg \subseteq Rf$.

**Definition.** Let $R$ be an integral domain. An element $u \in R$ is a unit if it has a multiplicative inverse in $R$, i.e. if there exists $v \in R$ such that $uv = 1$.

**Remark.** Recall that the set of units of $\mathbb{K}[x]$ is the group $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$ of nonzero elements of the field $\mathbb{K}$.

**Definition.** Let $R$ be an integral domain. Let $r$ be a nontrivial element of $R$ that is not a unit.

1. We say that $r$ is irreducible in $R$ if for any $r, s \in R$ 
   
   \[ r = st \Rightarrow \text{either } s \text{ or } t \text{ is a unit in } R. \]

2. We say that $r$ is a prime in $R$, if for any $s, t \in R$ 
   
   \[ r | st \text{ (in } R) \Rightarrow r | s \text{ or } r | t \text{ (in } R). \]

**Remark.** When $R = \mathbb{K}[x]$ we know that $\mathbb{K} \setminus \{0\}$ is the set of units. We can thus restate the definition of irreducibility as follows. Let $f$ be a polynomial in $\mathbb{K}[x]$ where $\deg f \geq 1$. We have that $f$ is irreducible in $\mathbb{K}[x]$ if for $g, h \in \mathbb{K}[x]$ 

\[ f = gh \Rightarrow \deg g = 0 \text{ or } \deg h = 0. \]

**Remark.** From Algebra 2B you know that $\mathbb{K}[x]$ is a principal ideal domain and that as a result the properties of being irreducible and a prime are equivalent. You also know that $\mathbb{K}[x]$ is a unique factorization domain.

Recall that a polynomial $0 \neq f \in \mathbb{K}[x]$ is said to be monic if the highest degree nonzero coefficient is 1.

**Remark.** Notice that if $\mathbb{K}$ is a field then all polynomials $ax + b \in \mathbb{K}[x]$ of degree 1 (and thus with $a \neq 0$) are irreducible.

**Unique factorization in $\mathbb{K}[x]$.** Let $0 \neq f \in \mathbb{K}[x]$. Then 

\[ f = uf_1f_2 \cdots f_n \]

where $n \geq 0$, $u \in \mathbb{K} \setminus \{0\}$ and $f_1, \ldots, f_n$ irreducible monic polynomials in $\mathbb{K}[x]$. Furthermore $u$ is unique and $f_1, \ldots, f_n$ are also unique up to order.

**Examples.** (1) $4x^4 - 16 = 4(x^2 - 2)(x^2 + 2)$ is the unique factorization of $4x^4 - 4$ in $\mathbb{Q}[x]$.

(2) The unique factorization in $\mathbb{R}[x]$ is 

\[ 4x^4 - 16 = 4(x - \sqrt{2})(x + \sqrt{2})(x^2 + 2). \]
(3) The unique factorization in \( \mathbb{C}[x] \) is
\[
4x^4 - 16 = 4(x - \sqrt{2})(x + \sqrt{2})(x - i\sqrt{2})(x + i\sqrt{2}).
\]

**Division with remainder.** If \( 0 \neq f, g \in \mathbb{K}[x] \). Then there exist \( r, s \in \mathbb{K}[x] \) such that
\[
f = gs + r
\]
and \( \deg r < \deg g \).

**Definition.** We say that an element \( t \in \mathbb{K} \) is a root of the polynomial \( f = a_0 + a_1x + \cdots + a_nx^n \) in \( \mathbb{K}[x] \) if
\[
f(t) = a_0 + a_1t + \cdots + a_nt^n = 0.
\]

**Lemma 1.2** Let \( \mathbb{K} \) be a field and let \( f \in \mathbb{K}[x] \). An element \( t \in \mathbb{K} \) is a root of \( f \) if and only if \( x - t \) divides \( f \) in \( \mathbb{K}[x] \).

**Proof** Suppose \( f(t) = 0 \). Using division with remainder we have
\[
f = (x - t)g + r
\]
where \( r \) is of degree less than 1 and thus in \( \mathbb{K} \). Now \( r = (t - t)g(t) + r = f(t) = 0 \) and thus \( f = (x - t)g \).

Conversely, if \( x - t \) divides \( f \), say \( f = (x - t)g \), then \( f(t) = (t - t)g(t) = 0 \) and \( t \) is a root of \( f \). \( \square \)

**Greatest common divisor and lowest common multiple.** Let \( 0 \neq f, g \in \mathbb{K}[x] \).

(1) An element \( d \in \mathbb{K}[x] \) is called a greatest common divisor (gcd) of \( f \) and \( g \) if:

(i) \( d \mid f \) and \( d \mid g \)

(ii) if \( r \mid f \) and \( r \mid g \) then \( r \mid d \).

2) An element \( c \in \mathbb{K}[x] \) is called a lowest common multiple (lcm) of \( f \) and \( g \) if:

(i) \( f \mid c \) and \( g \mid c \)

(ii) if \( f \mid r \) and \( g \mid r \) then \( c \mid r \).

**Remark.** (1) If \( d_1, d_2 \) are both greatest common divisors of \( f \) and \( g \), then \( d_2 = ud_1 \) for some \( 0 \neq u \in \mathbb{K} \). In particular there is a unique monic polynomial that is the greatest common divisor of \( f \) and \( g \).

(2) If \( c_1, c_2 \) are both lowest common multiples of \( f \) and \( g \), then \( c_2 = uc_1 \) for some \( 0 \neq u \in \mathbb{K} \). In particular there is a unique monic polynomial that is the lowest common multiple of \( f \) and \( g \).

(3) From Algebra 2B you know that
\[
\mathbb{K}[x]f + \mathbb{K}[x]g = \mathbb{K}[x]d,
\]
\[ \mathbb{K}[x]f \cap \mathbb{K}[x]g = \mathbb{K}[x]c. \]

**Remark.** In particular there exists polynomials \( r, s \in \mathbb{K}[x] \) such that
\[ rf + sg = d. \]

**IV. Criteria for irreducibility in \( \mathbb{Q}[x] \)**

**Remark** Everything we do in this in this section works also if we replace \( \mathbb{Z} \) by any principal ideal domain \( R \) and \( \mathbb{Q} \) by the field of fractions \( F \) for \( R \).

**Lemma 1.3 (Gauss).** Let \( p \) be a prime in \( \mathbb{Z} \) and \( f, g \in \mathbb{Z}[x] \). Then (in \( \mathbb{Z}[x] \))
\[ p | fg \Rightarrow p | f \text{ or } p | g. \]

**Proof** Suppose that
\[
\begin{align*}
fg &= a_0 + a_1x + \cdots + a_nx^n \\
f &= b_0 + b_1x + \cdots b_rx^r \\
g &= c_0 + c_1x + \cdots c_sx^s.
\end{align*}
\]

We argue by contradiction and suppose that \( p \) divides neither \( f \) nor \( g \). Let \( b_i, c_j \) be the earliest coefficients of \( f \) and \( g \) respectively that are not divisible by \( p \). Notice that
\[
a_{i+j} = b_0c_{i+j} + b_1c_{i+j-1} + \cdots + b_{i-1}c_{j+1} + b_ic_j + b_{i+1}c_{j-1} + \cdots + b_{i+j}c_0.
\]

Since \( p \) divides \( a_{i+j}, b_0, \ldots, b_{i-1}, c_0, \ldots, c_{j-1} \) it follows that \( p \) divides \( b_ic_j \). But as \( p \) is a prime we then get the contradiction that \( p \) divides either \( b_i \) or \( c_j \). \( \square \)

**Theorem 1.4** Let \( f \in \mathbb{Z}[x] \) be a polynomial where \( \deg f \geq 1 \). If \( f \) is irreducible in \( \mathbb{Z}[x] \), then \( f \) is also irreducible in \( \mathbb{Q}[x] \).

**Proof** We argue by contradiction and suppose that \( f \) is irreducible over \( \mathbb{Z} \) but not over \( \mathbb{Q} \). It follows that
\[ f = gh \]
for some polynomials \( g, h \in \mathbb{Q}[x] \) where \( g, h \) are of both of degree at least 1. By multiplying by a suitable positive integer
\[ n = p_1 \cdots p_r, \]
where \( p_1, \ldots, p_r \) are prime numbers, we get an equation
\[ p_1 \cdots p_rf = g_0h_0 \]
where \( g_0, h_0 \in \mathbb{Z}[x] \). We now use last lemma. As \( p_r \) divides \( g_0h_0 \) it must divide either \( g_0 \) or \( h_0 \). Cancelling out this prime on both sides we get
\[ p_1 \cdots p_{r-1}f = g_1h_1 \]
for some polynomials $g_1, h_1$ over $\mathbb{Z}$. (Notice that the degrees of $g_1, h_1$ are the same as the degrees of $g_0, h_0$ respectively). By repeating this we can eliminate the primes one by one and we arrive at

$$f = g_r h_r$$

where $g_r, h_r$ are polynomials over $\mathbb{Z}$ (and where $g_r, h_r$ have the same degrees as $g, h$). But this contradicts the assumption that $f$ was irreducible over $\mathbb{Z}$.

**Remark.** The converse is not true. For example the polynomial $f = 2x$ is irreducible in $\mathbb{Q}[x]$ but is not irreducible in $\mathbb{Z}[x]$ as 2 is not a unit in $\mathbb{Z}$. From the proof of last result we can also deduce the following.

**Corollary 1.5** Let $f \in \mathbb{Z}[x]$ and suppose that $f = g_1 g_2$ with $g_1, g_2 \in \mathbb{Q}[x]$. Then there exist polynomials $h_1, h_2 \in \mathbb{Z}[x]$ of same degrees as $g_1, g_2$ such that

$$f = h_1 h_2.$$
The polynomial $f = \frac{2}{9}x^5 + \frac{5}{3}x^4 + x^3 + \frac{1}{3}$ is irreducible over $\mathbb{Q}$ iff $9f = 2x^5 + 15x^4 + 9x^3 + 3$ is irreducible over $\mathbb{Q}$. By Eisenstein, using $p = 3$, the latter is irreducible.

We now turn to yet another irreducibility criteria. For a prime number $p$ in $\mathbb{Z}$ we consider the homomorphism

$$\phi: \mathbb{Z} \rightarrow \mathbb{Z}_p, \ a \mapsto \overline{a} = a + \mathbb{Z}_p.$$  

**Theorem 1.7** Let $p$ be a prime number and let

$$f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$$

where $\deg(f) = n \geq 1$ and where $p$ does not divide $a_n$. Consider the corresponding polynomial

$$\phi_p^*(f) = \overline{a}_0 + \overline{a}_1x + \cdots + \overline{a}_n x^n$$

over $\mathbb{Z}_p$. Then if $\phi_p^* f$ is irreducible in $\mathbb{Z}_p[x]$, $f$ is irreducible in $\mathbb{Q}[x]$.

**Proof** Argue by contractions and suppose that there exist $g, h \in \mathbb{Q}[x]$ of degrees at least 1 and where $f = gh$. By Corollary 1.5 we can assume that $g, h \in \mathbb{Z}[x]$. Then

$$\phi_p^*(f) = \phi_p^*(g) \cdot \phi_p^*(h)$$

is a factorization of $\phi_p^*(f)$ in $\mathbb{Z}_p[x]$ (notice that $\phi_p^*(f), \phi_p^*(g), \phi_p^*(h)$ have same degrees as $f, g, h$) that contradicts our assumption that $\phi_p^*(f)$ was irreducible in $\mathbb{Z}_p[x]$. $\square$.

**Example.** Show that $f = x^3 + 11x + 100$ is irreducible over $\mathbb{Q}$.

**Solution.** We have that $g = \phi_3^*(f) = x^3 + \overline{2}x + \overline{1} \in \mathbb{Z}_3[x]$ is irreducible as it has no root (and thus no linear factor). In fact $g(0) = g(1) = g(\overline{2}) = \overline{1}$. By last proposition it thus follows that $f$ is irreducible over $\mathbb{Q}$.
2 Field Extensions

I. Field extensions and their associated vector space and group

Definition. A field extension is a pair of two fields $K, F$ where $K$ is contained in $F$. We will use $K \subseteq F$ to denote the field extension.

The associated vector space. For a field extension $K \subseteq F$ we can view the larger field $F$ as a vector space over the subfield $K$. Here the vector space addition is the same as the field addition in $F$ and the scalar multiplication from $K$ is inherited from the field multiplication in $F$. One readily checks that all the vector space axioms hold (see Exercise Sheet 3).

Definition. Let $K \subseteq F$ be a field extension. The degree of the field extension, denoted $[F : K]$, is the dimension of $F$ viewed as a vector space over $K$.

Examples. (1) $C = \mathbb{R} \oplus \mathbb{R}i$ and thus $[C : \mathbb{R}] = 2$.
(2) $\mathbb{R}$ has uncountable basis as a vector space over $\mathbb{Q}$.
(3) Notice that every field can be viewed as a vector space over its prime subfield. Thus either a vector space over $\mathbb{Q}$ or a vector space over $\mathbb{Z}_p$.

Lemma 2.1 (The tower law). Let $K \subseteq M \subseteq F$ be an ascending chain of fields. Suppose that $(x_i)_{i \in I}$ is a basis for $M$ over $K$ and $(y_j)_{j \in J}$ is a basis for $F$ over $M$. Then $(x_iy_j)_{i \in I, j \in J}$ is a basis for $F$ over $K$. In particular we have that $[F : K] = [F : M] \cdot [M : K]$.

Proof To start with, we have $F = \sum_{j \in J} M y_j$ and $M = \sum_{i \in I} K x_i$. Therefore

$$F = \sum_{j \in J} \left( \sum_{i \in I} K x_i \right) y_j = \sum_{i \in I, j \in J} K x_i y_j$$

and $F$ is generated by $(x_iy_j)_{i \in I, j \in J}$ as a vector space over $K$. We need to prove linear independence. But if

$$0 = \sum_{i \in I, j \in J} a_{ij} x_i y_j = \sum_{j \in J} \left( \sum_{i \in I} a_{ij} x_i \right) y_j,$$

then $\sum_{i \in I} a_{ij} x_i = 0$ for all $j \in J$ as $(y_j)_{j \in J}$ is a basis for $F$ over $M$. But as $(x_i)_{i \in I}$ is a basis for $M$ over $K$ it then follows that $a_{ij} = 0$ for all $i \in I$ and $j \in J$. This finishes the proof. \(\square\)

The Galois group of a field extension. We will see that there is a natural group associated to any field extension. Let us first recall the definition of a group.
Definition. A group is a set $G$ equipped with a binary operation $\cdot$ such that

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$.
2. There exists $1 \in G$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in G$.
3. For each $a \in G$ there exists $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Definition. A subset $H$ of $G$ is a subgroup if $1 \in H$ and $ab, a^{-1} \in H$ whenever $a, b \in H$. We often use $H \leq G$ for ‘$H$ is a subgroup of $G$’.

Let $F$ be a field and let $\text{Aut}_F$ be the set of all ring automorphisms (that is isomorphisms) $\phi : F \to F$. Recall from Algebra 2B, that $\text{Aut}_F$ is a group with respect to composition (a subgroup of the group of all bijections $F \to F$).

Let $K \subseteq F$ be a field extension. Let

$$\text{Aut}_KF = \{ \phi \in \text{Aut}_F : \phi(a) = a \text{ for all } a \in K \}.$$ 

Lemma 2.2 $\text{Aut}_KF$ is a subgroup of $\text{Aut}_F$.

Proof Clearly $\text{id} : F \to F$ is in $\text{Aut}_KF$. It remains to see that $\text{Aut}_KF$ is closed under composition and taking inverses. Let $\phi, \psi \in \text{Aut}_KF$ then for every $a \in K$ we have

$$\psi \phi(a) = \psi(\phi(a)) = \psi(a) = a.$$ 

and

$$a = \phi^{-1}(\phi(a)) = \phi^{-1}(\phi(a)) = \phi^{-1}(a).$$

This shows that $\psi \phi$ and $\phi^{-1} \in \text{Aut}_KF$ that finishes the proof. □

Defintion. Let $K \subseteq F$ be a field extension. The group $\text{Aut}_KF$ is called the Galois group of the field extension.

Example. Consider the field extension $\mathbb{R} \subseteq \mathbb{C}$. Here $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$. Let $\sigma \in \text{Aut}_RC$. Now $\sigma$ fixes all the elements in $\mathbb{R}$ pointwise. As $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$ we have $\sigma(i) = \pm i$. Thus we have that $\text{Aut}_R\mathbb{C} = \langle \tau \rangle$, a cyclic group of order 2 where $\tau : \mathbb{C} \to \mathbb{C}, a+bi \mapsto a-ib$ is the conjugation map. This is a homomorphism as $\tau w = \tau \cdot w$ as well as $z + w = \tau + \overline{w}$.

Lemma 2.3 Let $K \subseteq M \subseteq F$ be an ascending chain of fields. Then $\text{Aut}_M\mathbb{F}$ is a subgroup of $\text{Aut}_KF$.

Proof As both $\text{Aut}_KF$ and $\text{Aut}_MF$ are groups it suffices to show that $\text{Aut}_M\mathbb{F} \subseteq \text{Aut}_KF$. If $\sigma \in \text{Aut}_MF$ then $\sigma$ fixes $M$ pointwise and hence also the subfield $K$. Thus $\sigma \in \text{Aut}_KF$. □

Let $H$ be a subgroup of $G = \text{Aut}_KF$. For every subgroup $H$ of $G$ we let

$$\text{Fix } H = \{ a \in F | \sigma(a) = a \text{ for all } \sigma \in H \}.$$ 

Lemma 2.4 Fix $H$ is a subfield of $F$ containing $K$.  

11
Proof To show that the subset \( \text{Fix} \ H \) of \( F \) is a subfield we need only to check that all the relevant closure properties hold. Clearly \( 1 \in \text{Fix} \ H \) (as \( 1 \in \mathbb{K} \)). If \( a, b \in \text{Fix} \ H \) and \( \sigma \in H \), then \( \sigma(a+b) = \sigma(a) + \sigma(b) = a + b, \sigma(ab) = \sigma(a)\sigma(b) = ab \) and \( \sigma(-a) = -\sigma(a) = -a \). Hence \( \text{Fix} \ H \) is closed under addition and multiplication as well as with respect to taking additive inverses. Furthermore if \( 0 \neq a \in \text{Fix} \ H \), then \( \sigma(a-1) = \sigma(a) - 1 = a - 1 \) and thus \( \text{Fix} \ H \) is also closed under taking multiplicative inverses of non-zero elements. This shows that \( \text{Fix} \ H \) is a subfield of \( F \). Finally as all elements in \( G \) fix \( \mathbb{K} \) pointwise (and thus all elements in \( H \) in particular), it is clear that \( \text{Fix} \ H \) contains \( \mathbb{K} \).

Let \( \mathbb{K} \subseteq F \) be a field extension. Let

\[
\mathcal{F} = \{ M : \mathbb{K} \leq M \leq F \}, \quad \text{and} \quad \mathcal{G} = \{ H : H \leq G = \text{Aut}_{\mathbb{K}}F \}.
\]

We introduce two maps

\[
\Phi : \mathcal{F} \rightarrow \mathcal{G}, \ M \mapsto \text{Aut}_M F
\]

and

\[
\Psi : \mathcal{G} \rightarrow \mathcal{F}, \ H \mapsto \text{Fix}(H).
\]

Notice that by Lemma 2.3 and Lemma 2.4 we know that the two maps are well defined. We will show later in the course that under certain restrictions these two maps will provide us with a close remarkable correspondence between the intermediate subfield structure of the field extension \( \mathbb{K} \subseteq F \) and the subgroup structure of its Galois group \( \text{Aut}_{\mathbb{K}}F \). Next lemma gives the first indication that there is a link between the two.

**Lemma 2.5** The maps \( \Psi \) and \( \Phi \) satisfy the following properties.

1. \( \Phi(M_1) \geq \Phi(M_2) \) when \( M_1 \leq M_2 \). Also \( \Psi(H_1) \geq \Psi(H_2) \) when \( H_1 \leq H_2 \).
2. \( H \leq \Phi(\Psi(H)) \) for all \( H \in \mathcal{G} \) and \( M \leq \Psi(\Phi(M)) \) for all \( M \in \mathcal{F} \).
3. \( \Phi(M) = \Phi(\Psi(\Phi(M))) \) for all \( M \in \mathcal{F} \) and \( \Psi(H) = \Psi(\Phi(\Psi(H))) \) for all \( H \in \mathcal{G} \).

**Proof.** See Exercise Sheet 3. \( \square \).

**II. Algebraic and transcendental elements**

**Definition.** Let \( \mathbb{K} \subseteq F \) be a field extension. An element \( a \in F \) is said to be **algebraic over** \( \mathbb{K} \) if there is a non-zero polynomial \( f \in \mathbb{K}[X] \) such that \( f(a) = 0 \). Otherwise we say that \( a \) is **transcendental over** \( \mathbb{K} \).

**Examples.** As \( \sqrt{2} \) is the root in \( \mathbb{R} \) of \( f = x^2 - 2 \in \mathbb{Q}[x] \), \( \sqrt{2} \) is algebraic over \( \mathbb{Q} \). On the other hand \( \pi \in \mathbb{R} \) isn’t the root of any polynomial in \( \mathbb{Q}[x] \) and thus \( \pi \) is transcendental over \( \mathbb{Q} \).

**The smallest subring** of \( F \) **containing** \( \mathbb{K} \) **and** \( a \in F \).

Let \( \mathbb{K} \subseteq F \) be a field extension and let \( a \in F \). Any subring of \( F \) that contains \( \mathbb{K} \) and \( a \) must contain all polynomial expressions

\[
\mathbb{K}[a] = \{ f(a) : f \in \mathbb{K}[x] \}.
\]
Notice that $\mathbb{K}[a]$ is the image of the ring homomorphism $\phi: \mathbb{K}[x] \rightarrow \mathbb{F}$, $f \mapsto f(a)$ and thus $\mathbb{K}[a]$ is a subring of $\mathbb{F}$. This is clearly the smallest subring of $\mathbb{F}$ that contains $\mathbb{K}$ and $a$. We are now going to analyse the structure of the smallest subfield of $\mathbb{F}$ containing $\mathbb{K}$ and $a$. Denote this subfield by $\mathbb{K}(a)$.

**Case 1** (a transcendental over $\mathbb{K}$). This is quite straightforward. As $a$ is not a root of any non-zero polynomial we have that the ring homomorphism $\phi$ above is injective. Thus $\mathbb{K}[a] \cong \mathbb{K}[x]$, the ring of polynomials in one variable over $\mathbb{K}$. Let $\mathbb{K}(x) = \{f/g : f, g \in \mathbb{K}[x] \text{ and } g \neq 0\}$. be the field of all rational expressions in one variable. We can use $\phi$ to obtain an injective ring homomorphism

$$
\psi: \mathbb{K}(x) \rightarrow \mathbb{F}, \ f/g \mapsto f(a)/g(a).
$$

The image is clearly the smallest subfield of $\mathbb{F}$ containing $\mathbb{K}$ and $a$. Thus $\mathbb{K}(a) \cong \mathbb{K}(x)$. (See Exercise sheet 3 for more details).

**Case 2**. (a algebraic over $\mathbb{K}$).

**Proposition 2.6** Let $\mathbb{K} \subseteq \mathbb{F}$ be a field extension and let $a \in \mathbb{F}$ be algebraic over $\mathbb{K}$.

1. $\mathbb{K}(a) = \mathbb{K}[a] \cong \mathbb{K}[x]/\mathbb{K}[x]f$ for a unique irreducible monic polynomial $f \in \mathbb{K}[x]$.

2. Let $n = \deg f$. Then $(1, a, a^2, \ldots, a^{n-1})$ is a basis for $\mathbb{K}(a)$ as a vector space over $\mathbb{K}$.

Thus

$$
\mathbb{K}(a) = \mathbb{K} \oplus \mathbb{K}a \oplus \cdots \mathbb{K}a^{n-1}
$$

and $[\mathbb{K}(a) : \mathbb{K}] = \deg f$.

**Proof** (1) Consider the ring homomorphism $\phi: \mathbb{K}[x] \rightarrow \mathbb{F}$, $f \mapsto f(a)$. As $\mathbb{K}[x]$ is a PID, $\ker \phi = \mathbb{K}[x]f$ for some polynomial $f \in \mathbb{K}[x]$ that is of degree at least 1 as $a$ is algebraic over $\mathbb{K}$. Furthermore $f$ is unique provided we further require that it is monic (if there was another such polynomial monic polynomial then $g - f$ would be a non-trivial polynomial in $\mathbb{K}[x]/f$ of degree less than $\deg f$ but this is absurd). To see why $f$ must be irreducible in $\mathbb{K}[x]$, we argue by contradiction and suppose that $f = gh$ where $1 \leq \deg g, \deg h < \deg f$.

But then

$$
0 = f(a) = g(a)h(a)
$$

and as $\mathbb{F}$ is a field we must have either $g(a) = 0$ or $h(a) = 0$. But then one of $h, g$ is in $\ker \phi = \mathbb{K}[x]f$ and thus divisible by $f$. Again this is absurd. By the first isomorphism theorem $\mathbb{K}[a] \cong \mathbb{K}[x]/\mathbb{K}[x]f$.

From this one can deduce that $\mathbb{K}[a]$ is a field. Let $0 \neq g(a) \in \mathbb{K}[a]$. As $f$ is irreducible and as $f$ does not divide $g$ in $\mathbb{K}[x]$, we have that $f$ and $g$ are coprime and we thus have

$$
1 = fr + gs
$$

for some $r, s \in \mathbb{K}[x]$. But then $1 = f(a)r(a) + g(a)s(a) = 0 \cdot r(a) + g(a)s(s) = g(a)s(a)$.

This shows that $g(a)$ has a multiplicative inverse $s(a) \in \mathbb{K}[a]$. We have thus shown that $\mathbb{K}[a]$ is a field and thus the smallest subfield containing $a$ and $\mathbb{K}$. Hence $\mathbb{K}(a) = \mathbb{K}[a]$.

(2) Let $g(a) \in \mathbb{K}[a]$ for some $g \in \mathbb{K}[x]$. Using division with remainder there exist
If \( q, r \in \mathbb{K}[x] \) such that \( g =fq+r \) and where \( \deg r < \deg f \), say \( r = b_0 + b_1 x + \ldots + b_{n-1} x^{n-1} \). Then
\[
g(a) = f(a)q(a) + r(a) = 0 \cdot q(a) + r(a) = b_0 + b_1 a + \ldots + b_{n-1} a^{n-1}
\]
and we thus have \( g(a) \in \mathbb{K} + \mathbb{K} a + \ldots + \mathbb{K} a^{n-1} \). It remains only to show that \( 1, a, \ldots, a^{n-1} \) are linearly independent. Suppose
\[
b_0 + b_1 a + \ldots + b_{n-1} a^{n-1} = 0.
\]
Then \( g = b_0 + b_1 x + \ldots + b_{n-1} x^{n-1} \in \ker \phi = \mathbb{K}[x] f \). As \( \deg f > \deg g \), this can only happen if \( g = 0 \) that is if \( b_0, \ldots, b_{n-1} = 0 \). This shows that \( 1, a, \ldots, a^{n-1} \) are linearly independent. \( \square \)

**Remark.** Notice that the structure of \( \mathbb{K}[a] \) only depends on \( \mathbb{K}[x] \) and \( f \). The addition is just like addition of polynomials
\[
(b_0 + b_1 a + \ldots + b_{n-1} a^{n-1}) + (c_0 + c_1 a + \ldots + c_{n-1} a^{n-1}) = (b_0 + c_0) + (b_1 + c_1) a + \ldots + (b_{n-1} + c_{n-1}) a^{n-1}
\]
and the multiplication is just like multiplication of polynomials but where we then use \( f(a) = 0 \), that is
\[
a^n = -(a_0 + a_1 a + \ldots + a_{n-1} a^{n-1})
\]
to reduce the polynomial expression to something of degree at most \( n - 1 \).

**Examples.** Consider the field extension \( \mathbb{Q} \subseteq \mathbb{C} \). We have that the relevant polynomials for \( i, \sqrt{2} \) and \( \sqrt[3]{2} \) are \( x^2 + 1, x^2 - 2 \) and \( x^3 - 2 \). Here thus
\[
\begin{align*}
\mathbb{Q}(i) &= \mathbb{Q} \oplus \mathbb{Q} i \\
\mathbb{Q}(\sqrt{2}) &= \mathbb{Q} \oplus \mathbb{Q} \sqrt{2} \\
\mathbb{Q}(\sqrt[3]{2}) &= \mathbb{Q} \oplus \mathbb{Q} \sqrt[3]{2} \oplus \mathbb{Q}(\sqrt[3]{2})^2.
\end{align*}
\]
Here for example \( i^2 = -1 \) and thus \( (2 - i)(1 + 2i) = 2 + 3i - 2i^2 = 2 + 3i + 2 = 4 + 3i \). For \( a = \sqrt[3]{2} \), we have \( a^3 = 2 \) and thus
\[
(1 + \sqrt[3]{2})(1 - (\sqrt[3]{2})^2) = (1 + a)(1 - a^2) = 1 + a - a^2 - a^3 = -2 + a - a^2 = -2 + \sqrt[3]{2} - (\sqrt[3]{2})^2.
\]

**Definition.** Let \( \mathbb{K} \subseteq \mathbb{F} \) be a field extension and let \( a \) be an element in \( \mathbb{F} \) that is algebraic over \( \mathbb{K} \). The **minimal polynomial of \( a \)** over \( \mathbb{K} \) is the monic polynomial \( m_a \in \mathbb{K}[x] \) of smallest degree such that \( m_a(a) = 0 \).

**Remark.** We have shown above that \( m_a \) is irreducible over \( \mathbb{K} \) and unique and that \( m_a \) divides any polynomial \( g \in \mathbb{K}[x] \) where \( g(a) = 0 \).

**Example.** The minimal polynomial of \( \sqrt[3]{-1} \) in \( \mathbb{R} \) over \( \mathbb{Q} \) is \( (x+1)^3-3 = x^3+3x^2+3x-2 \).

**Definition.** Let \( \mathbb{K} \subseteq \mathbb{F} \) be a field extension. If there exists \( a \in \mathbb{F} \) such that \( \mathbb{F} = \mathbb{K}(a) \), then we say that \( \mathbb{K} \subseteq \mathbb{F} \) is a **simple extension**. The degree of the extension \( [\mathbb{K}(a) : \mathbb{K}] \) is sometimes also called the **degree of \( a \)** over \( \mathbb{K} \).
Remark. We have just observed that the structure of $\mathbb{K}(a) = \mathbb{K}[a]$ just depends on $\mathbb{K}[x]$ and the minimal polynomial of $a$ over $\mathbb{K}$. In fact this is also clear from the isomorphism $\mathbb{K}(a) \cong \mathbb{K}[x]/\mathbb{K}[x]m_a$. This provides us with a clue as to how we can, for any irreducible polynomial $f$, construct a field $\mathbb{F}$ such that $\mathbb{F} = \mathbb{K}(a)$ and $f(a) = 0$. Let us first recall why $\mathbb{K}[x]/\mathbb{K}[x]f$ is a field in this case.

**Lemma 2.7** Let $f$ be an irreducible polynomial in $\mathbb{K}[x]$. We have that $\mathbb{K}[x]/\mathbb{K}[x]f$ a field.

**Proof** Let $\bar{0} \neq \bar{a} \in \mathbb{K}[x]/\mathbb{K}[x]f$. Then $f$ does not divide $a$ and thus $a$ and $f$ have no common irreducible factor. It follows that $a$ and $f$ are coprime and $1 = ra + sf$ for some polynomials $r, s \in \mathbb{K}[x]$. We thus have

$$\bar{1} = \bar{r}\bar{a} + \bar{s}\bar{f} = \bar{r}\bar{a} + \bar{s}\bar{0} = \bar{r}\bar{a}.$$ 

So $\bar{a}$ has an inverse $\bar{r}$. This shows that any non-zero element in $\mathbb{K}[x]/\mathbb{K}[x]f$ has a multiplicative inverse. Hence $\mathbb{K}[x]/\mathbb{K}[x]f$ is a field. $\square$

**Remark.** Recall from Algebra 2B that we can think of $\mathbb{K}[x]/\mathbb{K}[x]f$ naturally as a vector space over $\mathbb{K}$ where the scalar multiplication is

$$ag = \bar{a}\bar{g}$$

for $a \in \mathbb{K}$ and $g \in \mathbb{K}[x]$.

**Proposition 2.8** Let $f$ be an irreducible polynomial in $\mathbb{K}[x]$ of degree $n$ and let $\mathbb{F}$ be the field $\mathbb{K}[x]/\mathbb{K}[x]f$. Let $1_{\mathbb{F}} = \bar{1}$ be the multiplicative identity of $\mathbb{F}$ and let $t = \bar{x} = x + \mathbb{K}[x]f$. Then

$$\mathbb{F} = \mathbb{K}1_{\mathbb{F}} \oplus \mathbb{K}t \oplus \cdots \oplus \mathbb{K}t^{n-1}.$$ 

Furthermore $f(t) = 0$.

**Proof** Let $\bar{g} = g + \mathbb{K}[x]$ be an arbitrary element in $\mathbb{F}$ where $g \in \mathbb{K}[x]$. Using division with remainder we get

$$g = fs + r$$

for some polynomial $b_0 + b_1x + \cdots + b_{n-1}x^{n-1} \in \mathbb{K}[x]$ of degree less than $n$. Hence (as $f = 0$)

$$\bar{g} = \bar{f}\bar{s} + \bar{b}_0\bar{1} + \bar{b}_1\bar{x} + \cdots + \bar{b}_{n-1}(\bar{x})^{n-1} = \bar{b}_01_{\mathbb{F}} + \bar{b}_1t + \cdots + \bar{b}_{n-1}t^{n-1}.$$ 

This shows that $1_{\mathbb{F}}, t, t^2, \ldots, t^{n-1}$ generate $\mathbb{F}$ as a vector space over $\mathbb{K}$. Let us see why they are linearly independent. Suppose $b_01_{\mathbb{F}} + b_1t + \cdots + b_{n-1}t^{n-1} = 0$. This is the same as saying that $\bar{g} = \bar{0}$ or equivalently that $g \in \mathbb{K}[x]f$ where $g = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$. But as the degree of $g$ is less than the degree of $f$ this can only happen when $g = 0$, that is when $b_0 = b_1 = \ldots = b_{n-1} = 0$.

Finally if $f = a_0 + a_1x + \cdots + a_nx^n$. Then

$$f(t) = a_01_{\mathbb{F}} + a_1t + \cdots + a_nt^n = a_0\bar{1} + a_1\bar{x} + \cdots + a_n(\bar{x})^n = a_0 + \bar{a}_1x + \cdots + \bar{a}_nx^n = \bar{f} = \bar{0} = 0_{\mathbb{F}}.$$
This finishes the proof. □

Remarks. (1) This gives us a field extension \( K_1 \subseteq F \) where \( K_1 \cong K \) (See Exercise sheet 4 for some clarifications). We should thus perhaps more naturally consider \( t \) as a root of the polynomial

\[
a_0 1_F + a_1 1_F x + \cdots + a_n 1_F x^n
\]

in \( K_1[x] \). We then have concretely constructed a simple field extension \( K_1 \subseteq K_1(t) \).

This is however an unnecessary formalism. We simply identify \( a \in K \) with \( a 1_F \) in \( K_1 \) and think of \( K \) itself as a subfield of \( F \). Then our simple field extension is \( K \subseteq K(t) \) and our polynomial can remain exactly what it was.

(2) Let \( f \) be any polynomial in \( K[x] \) of degree at least 1 and let \( q \) be any irreducible factor, say \( f = qg \). Proposition 2.8 gives us a larger field where \( q \) has a root \( t \). But then \( f(t) = q(t)g(t) = 0g(t) = 0 \) and thus \( f \) has a root in a larger field.

Examples (1) Consider \( \mathbb{Q} \subseteq \mathbb{Q}(i) \). Now the minimal polynomial of \( i \) over \( \mathbb{Q} \) is \( x^2 + 1 \). By Proposition 2.6 we then have

\[
\mathbb{Q}(i) = \mathbb{Q} \oplus \mathbb{Q}i
\]

where the field operations are like adding and multiplying polynomial expressions and using \( i^2 + 1 = 0 \).

(2) Consider the irreducible polynomial \( x^2 + 1 \in \mathbb{Q}[x] \). Using Proposition 2.8, we get a field extension \( \mathbb{Q} \subseteq \mathbb{Q}(t) \) where

\[
\mathbb{Q}(t) = \mathbb{Q} \oplus \mathbb{Q}t
\]

where again the field operations are like adding and multiplying polynomial expressions and using \( t^2 + 1 = 0 \). Of course \( \mathbb{Q}(t) \) and \( \mathbb{Q}(i) \) are isomorphic.

(2) Consider the irreducible polynomial \( x^2 + x + 1 \in \mathbb{Z}_2[x] \). Using Proposition 2.8 we can then construct a new field

\[
\mathbb{F} = \mathbb{Z}_2(t) = \mathbb{Z}_2 \oplus \mathbb{Z}_2t,
\]

where \( t^2 = t + 1 \). We have thus constructed a field with 4 elements.

III. Algebraic field extensions

Let \( K \subseteq F \) be a field extension and let \( a_1, \ldots, a_n \in F \). Consider the ring homomorphism

\[
K[x_1, \ldots, x_n] \rightarrow F, \ f \mapsto f(a_1, \ldots, a_n).
\]

The image, denoted by \( K[a_1, \ldots, a_n] \), is the smallest subring of \( F \) that contains \( K \) and \( a_1, \ldots, a_n \). The subfield

\[
K(a_1, \ldots, a_n) = \{ a/b : a, b \in K[a_1, \ldots, a_n], b \neq 0 \}
\]

is the smallest subfield of \( F \) that contains \( K \) and \( a_1, \ldots, a_n \).

Remark. Clearly \( K(a_1, \ldots, a_n) = K(a_1)(a_2) \cdots (a_n) \).
Definition. Let $K \subseteq F$ be a field extension.

(1) We say that $K \subseteq F$ is **finitely generated** if there are finitely many elements $a_1, \ldots, a_n \in F$ such that $F = K(a_1, \ldots, a_n)$.

(2) We say that $K \subseteq F$ is **finite** if $[F : K] < \infty$.

Remark. (2) is generally stronger than (1). For example $\mathbb{Q} \subseteq \mathbb{Q}(\pi)$ is clearly finitely generated but it is not finite. If 

$$\sum_{m=0}^{\infty} a_m \pi^m = 0$$

where almost all but not all the coefficients are zero, then this would imply that $\pi$ is algebraic. This we know is not the case and hence $1, \pi, \pi^2, \ldots$ are infinitely many linearly independent elements in $\mathbb{Q}(\pi)$ and thus $\mathbb{Q}(\pi)$ is infinitely dimensional over $\mathbb{Q}$. Likewise if we consider the field $F = \mathbb{Q}(x)$ of rational expressions in the free variable $x$, then $\mathbb{Q} \subseteq F$ is simple and thus finitely generated. It is however not finite. (In fact we know that $\mathbb{Q}(\pi)$ and $\mathbb{Q}(x)$ are isomorphic).

Definition. An extension $K \subseteq F$ is said to be **algebraic** if every element $a \in F$ is algebraic over $K$.

Theorem 2.9 Let $K \subseteq F$ be a field extension. The following are equivalent.

(1) $K \subseteq F$ is finite.

(2) There exist finitely many elements $a_1, \ldots, a_n \in F$ that are algebraic over $K$ and such that $F = K(a_1, \ldots, a_n)$.

(3) $K \subseteq F$ is finitely generated and algebraic.

Proof ((1) $\Rightarrow$ (3)). Suppose $[F : K] = n$ and let $a_1, \ldots, a_n$ be a basis for the vector space $F$ over $K$. Then clearly $F = K(a_1, \ldots, a_n)$ and thus the extension is finitely generated. To see that it is algebraic let $t \in F$. Then the $n + 1$ elements $1, t, \ldots, t^n$ are linearly dependent, say

$$b_0 + b_1 t + \cdots + b_n t^n = 0,$$

for some $b_0, \ldots, b_n \in K$ (not all zero). Thus $t$ is a root of the nonzero polynomial $f = b_0 + \cdots + b_n \pi^n$ over $K$. This shows that the extension is algebraic.

((3) $\Rightarrow$ (2)). This is obvious.

((2) $\Rightarrow$ (1)). Let $K_r = K(a_1, \ldots, a_r)$. Then $K_{k+1} = K_k(a_{k+1})$. By our assumption $a_{k+1}$ is algebraic over $K$ and thus also over the larger field $K_k$ (a nonzero polynomial in $K_k[x]$, mapping $a_{k+1}$ to zero is also in $K_k[x]$). By Proposition 2.6 we have that $[K_{k+1} : K_k] = [K_k(a_{k+1}) : K_k]$ is finite (same as the degree of the minimal polynomial $m_{k+1}$ of $a_{k+1}$ over $K_k$). Thus the the tower law gives

$$[F : K] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_1 : K_0] < \infty.$$
Corollary 2.10 Let $K \subseteq M \subseteq F$ be an ascending chain of fields. Then $K \subseteq F$ is algebraic if and only if $K \subseteq M$ and $M \subseteq F$ are algebraic.

Proof ($\Rightarrow$) Suppose $K \subseteq F$ is algebraic. To see that $K \subseteq M$ is algebraic notice that every element in $M$ is in $F$ and thus algebraic over $K$. Now we turn to $M \subseteq F$. Let $a \in F$. As $a$ is algebraic over $K$ there is some $0 \neq f \in K[x]$ such that $f(a) = 0$. But as $K \subseteq M$, $f$ is also in $M[x]$ and thus $a$ algebraic over $M$.

($\Leftarrow$) Let $a \in F$. As $M \subseteq F$ is algebraic there is a polynomial $0 \neq f \in M[x]$ with $a$ as a root. Suppose

$$f = b_nx^n + b_{n-1}x^{n-1} + \cdots + b_0,$$

with $b_0, \ldots, b_n \in M$. Then in fact $f \in K(b_0, \ldots, b_n)[x]$ and thus $a$ algebraic over $K(b_0, \ldots, b_n)$. Thus the extension $K(b_0, \ldots, b_n) \subseteq K(b_0, \ldots, b_n, a)$ is finite by Proposition 2.6 (the degree of the extension is the same as the degree of the minimal polynomial of $a$ over $K(b_0, \ldots, b_n)$). But as $b_0, \ldots, b_n \in M$, and thus algebraic over $K$, $K \subseteq K(b_0, \ldots, b_n)$ is finite by Theorem 2.9. Hence, using the tower law,

$$[K(b_0, \ldots, b_n, a) : K] = [K(b_0, \ldots, b_n, a) : K(b_0, \ldots, b_n)] \cdot [K(b_0, \ldots, b_n) : K] < \infty.$$

In particular it then follows from Theorem 2.9 that $a$ is algebraic over $K$. □

Corollary 2.11 Let $K \subseteq F$ be a field extension. Then

$$A_F/K = \{a \in F : a \text{ is algebraic over } K\}$$

is a subfield of $F$ containing $K$.

Proof It is clear that $K$ is contained in $A_F/K$ as any element $a \in K$ is algebraic over $K$ (it is root of the polynomial $x - a \in K[x]$). It remains to see that $A_F/K$ is a subfield of $F$. For this we only need to show that it is closed under taking addition, multiplication, taking additive inverses and taking multiplicative inverses of non-zero elements. To see this notice that if $a, b \in A_F/K$ then $a + b, ab, -a$, as well as $a^{-1}$, when $a \neq 0$ are in $K(a, b)$. As $a, b$ are algebraic over $K$, Theorem 2.9 tells us that $K \subseteq K(a, b)$ is algebraic. Thus in particular $a + b, ab, -a, a^{-1}$ are algebraic over $K$ and thus in $A_F/K$. □

Definition. $A_F/K$ is called the subfield of algebraic elements in $F$ over $K$.

IV. Splitting fields.

Suppose that $f \in K[x]$ is a polynomial of degree $n \geq 1$. We can factorise it into a product of irreducible polynomials over $K[x]$, say

$$f = p_1 \cdots p_r.$$

By Proposition 2.8, $p_1$ has a root $t_1$ in a larger field $K_1$. Now factorise $f$ over $K_1$ into a product of irreducibles over $K_1$

$$f = (x - t_1)q_2 \cdots q_s.$$
Again we can apply Proposition 2.8 to find a root \( t_2 \) in a larger field \( \mathbb{K}_2 \) and then we factorise into irreducibles over \( \mathbb{K}_2 \), say
\[
 f = (x - t_1)(x - t_2)h_3 \cdots k_i.
\]
Continuing in this manner we arrive (after \( n \) steps) to a larger field \( F \) over which \( f \) splits into linear factors
\[
 f = c(x - t_1) \cdots (x - t_n).
\]
with \( c \in \mathbb{K} \) and \( t_1, \ldots, t_n \in F \).

**Definition.** Let \( \mathbb{K} \) be a field and \( 0 \neq f \in \mathbb{K}[x] \). A field \( F \) that contains \( \mathbb{K} \) is called a splitting field of \( f \) over \( \mathbb{K} \) if

(a) \( f \) splits into linear factors over \( F \), that is
\[
 f = c(x - t_1) \cdots (x - t_n)
\]
with \( c \in \mathbb{K} \) and \( t_1, \ldots, t_n \in F \).

(b) \( F = \mathbb{K}(t_1, \ldots, t_n) \).

We have seen that a splitting field for \( f \) exists. We will next see that they all look the same. In fact we will need something slightly stronger later in the course and so our setting is going to be a bit more general.

**Lemma 2.12** Suppose \( \phi : \mathbb{K}_1 \to \mathbb{K}_2 \) is a field isomorphism. Let \( f_1 \in \mathbb{K}_1[x] \) be an irreducible polynomial over \( \mathbb{K}_1 \) and let \( f_2 = \phi^*(f_1) \). Let \( a_i \) be a root of \( f_i \) in some larger field \( F_i \). Then there is an isomorphism
\[
 \psi : \mathbb{K}_1(a_1) \to \mathbb{K}_2(a_2)
\]
such that \( \psi(a_1) = a_2 \) and \( \psi(a) = \phi(a) \) for all \( a \in \mathbb{K}_1 \).

**Proof** We know from Proposition 2.6 that \( \mathbb{K}_1(a_1) \) consists of polynomial expressions \( f(a_1) \) where \( f \) runs through the polynomial ring \( \mathbb{K}_1[x] \). Likewise \( \mathbb{K}_2(a_2) \) consists of polynomial expressions \( a_2 \) over \( \mathbb{K}_2 \). We define \( \psi : \mathbb{K}_1(a_1) \to \mathbb{K}_2(a_2) \) by \( \psi(f(a_1)) = \phi^*(f)(a_2) \) for any \( f \in \mathbb{K}_1[x] \). Thus
\[
 \psi(s_0 + s_1a_1 + \cdots + s_na_1^n) = \phi(s_0) + \phi(s_1)a_2 + \cdots + \phi(s_n)a_2^n.
\]
Clearly \( \psi(s) = \phi(s) \) for all \( s \in \mathbb{K}_1 \) and \( \psi(a_1) = a_2 \). It remains to see that \( \psi \) is a well defined field isomorphism. As \( \phi \) is bijective it is clear that all polynomial expressions in \( a_2 \) over \( \mathbb{K}_2 \) are covered by \( \psi \) and thus \( \psi \) is surjective.

\( \psi \) is well defined and injective. By Exercise 1 on sheet 2, we know that \( f_2 \) is irreducible over \( \mathbb{K}_2 \) and thus \( f_1, f_2 \) are the minimal polynomials of \( a_1, a_2 \). We have
\[
 f(a_1) = g(a_1) \iff f_1|(f - g)
\]
\[
 \iff f_2 = \phi^*(f_1)|(\phi^*(f) - \phi^*(g))
\]
\[
 \iff \phi^*(f)(a_2) = \phi^*(g)(a_2)
\]
\[
 \iff \psi(f(a_1)) = \psi(g(a_1)).
\]
\( \psi \) is a ring homomorphism. This follows from the already established fact that \( \phi^* : K_1[x] \to K_2[x] \) is a ring homomorphism. □

**Remark.** Last lemma is intuitively kind of obvious. Suppose that the minimal polynomials have degree \( m \). Then

\[
K_1(a_1) = K_1 \oplus K_1a_1 \oplus \cdots \oplus K_1a_1^{m-1}
\]

and

\[
K_2(a_2) = K_2 \oplus K_2a_2 \oplus \cdots \oplus K_2a_2^{m-1}.
\]

The structure of the \( K_1(a_1) \) only depends on \( K_1[x] \) and \( f_1 \) and likewise the structure of \( K_2(a_2) \) only depends on \( K_2[x] \) and \( f_2 = \phi^*(f_1) \). As \( K_2 \) is just another copy of the field \( K_1 \) we have that \( K_2[x] \) is like \( K_1[x] \) and the polynomial \( f_2 \) is just like \( f_1 \) where we have just replaced the coefficients in \( f_1 \) with the corresponding coefficients in \( K_2 \).

**Theorem 2.13 (Uniqueness of the splitting field)** Suppose \( \phi : K_1 \to K_2 \) is a field isomorphism. Let \( f_1 \in K_1[x] \) be of degree at least one and let \( f_2 = \phi^*(f_1) \). Let \( F_i \) be a splitting field of \( f_i \) over \( K_i \). Then there exists a field isomorphism \( \psi : F_1 \to F_2 \) such that \( \psi(a) = \phi(a) \) for all \( a \in K_1 \).

**Proof** Suppose

\[
f_1 = c(x - a_1) \cdots (x - a_n)
\]

with \( c \in K_1 \) and \( a_1, \ldots, a_n \in F_1 \). Let \( g_1 \) be the minimal polynomial of \( a_1 \) over \( K_1 \). Then \( g_1|f_1 \) in \( K_1[x] \). Let \( b_1 \) be a root in \( F_2 \) of the factor \( \phi^*(g_1) \) of \( f_2 = \phi^*(f_1) \). By Lemma 2.12, there is an isomorphism

\[
\phi_1 : K_1(a_1) \to K_2(b_1)
\]

such that \( \phi_1(a_1) = b_1 \) and \( \phi_1(a) = \phi(a) \) for all \( a \in K_1 \). Now let \( g_2 \) be the minimal polynomial of \( a_2 \) over \( K_1(a_1) \). As before it is clear that \( g_2 \) divides \( f_1 \) and thus \( \phi_1^*(g_2)|\phi_1^*(f_1) = f_2 \). Let \( b_2 \) be a root of \( \phi_1^*(g_2) \) in \( F_2 \). Applying Lemma 2.12 again, there is a field isomorphism

\[
\phi_2 : K_1(a_1, a_2) \to K_2(b_1, b_2)
\]

such that \( \phi_2(a_2) = b_2 \) and \( \phi_2(a) = \phi_1(a) \) for all \( a \in K_1(a_1) \). Continuing in this manner we arrive at a isomorphism

\[
\psi : K_1(a_1, \ldots, a_n) \to K_2(b_1, \ldots, b_n)
\]

such that \( \psi(a_i) = b_i \) and \( \psi(a) = \phi(a) \) for all \( a \in K_1 \).

Now let \( d = \phi(c) \). Then

\[
d(x - b_1) \cdots (x - b_n) = \psi^*(c(x - a_1) \cdots (x - a_n)) = \psi^*(f_1) = \phi^*(f_1) = f_2
\]

Hence \( b_1, \ldots, b_n \) are the roots of \( f_2 \) in \( F_2 \) and \( F_2 = K_2(b_1, \ldots, b_n) \). We have thus shown that \( \psi \) is the isomorphism we were after. □

**Corollary 2.14** Let \( f \in K[x] \) be a polynomial of degree at least 1. Let \( F_1, F_2 \) be splitting fields of \( f \) over \( K \). There exists a field isomorphisms \( \psi : F_1 \to F_2 \) such that \( \psi(a) = a \) for all \( a \in K \).
**Proof.** Let $K_1 = K_2 = K$ and $\phi = \text{id}$ in Theorem 2.13. □

**Remark.** Let $F$ be a finite field. Then we see on sheet 4 that $|F| = p^n$ for some prime $p$ and positive integer $n$. Our next result is a remarkable application of Corollary 2.14. It gives us a classification of finite fields.

**Theorem 2.15** For each prime $p$ and positive integer $n$, there exists (up to isomorphism) exactly one field of order $p^n$. This is a splitting field of the polynomial $x^{p^n} - x$ over $\mathbb{Z}_p$.

**Proof** Let $F$ be a field of order $p^n$. Then $F \setminus \{0\}$ is a group of order $p^n - 1$. By Lagrange’s Theorem we then know that $a^{p^n-1} = 1$ for all $a \in F \setminus \{0\}$. Hence all the nontrivial elements of $F$ are roots of $x^{p^n} - x = x(x^{p^n-1} - 1)$. Of course the same is true for $0 \in F$. It follows that $F$ is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$. As all splitting fields of a given polynomial are isomorphic it follows that any two fields of the same order are isomorphic.

We still have some work to do as we want to show that all prime powers $p^n$ are covered. In order to do this we take arbitrary prime $p$ and positive integer $n$ and let $F$ be a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$. On problem sheet 5 we will see that the roots of the polynomial form a subfield of $F$ of order $p^n$. Hence $|F| = p^n$. □

We end this chapter by considering the Galois group of $K \subseteq F$ in the case when $F$ is the splitting field of some polynomial $f \in K[x]$.

**Lemma 2.16** Suppose $K_1 \subseteq F_1$ and $K_2 \subseteq F_2$ are field extensions. Suppose $\psi : F_1 \to F_2$ is a field isomorphism where $\psi(K_1) = K_2$. Let $f_1 \in K_1[x]$ and let $f_2 = \psi^*(f_1)$. If $a$ is a root of $f \in K_1[x]$ in $F_1$ then $\psi(a)$ is a root of $\psi^*(f) \in K_2[x]$ in $F_2$.

**Proof** Suppose $f = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$. Then $\psi^*(f) = \psi(\alpha_0) + \psi(\alpha_1)x + \cdots + \psi(\alpha_n)x^n$. Hence $\psi^*(f)(\psi(a)) = \psi(\alpha_0) + \psi(\alpha_1)\psi(a) + \cdots + \psi(\alpha_n)\psi(a)^n = \psi(\alpha_0 + \alpha_1 a + \cdots + \alpha_n a^n) = \psi(0) = 0$. □

**Remark**. In fact we are mostly interested in the special case when $K_1 = K_2$ and $\Psi$ fixes all the elements in $K$.

**Corollary 2.17** Suppose $K \subseteq F$ is a field extension and let $\sigma \in \text{Aut}_K F$. Let $a$ be a root of some polynomial $f \in K[x]$ of degree at least one. Then $\sigma(a)$ is also a root of $f$.

**Proof**. It is worth rewriting the proof for this special case. As $\sigma$ is a field automorphism that fixes the elements in $K$ pointwise it fixes all the coefficients of $f \in K[x]$. Suppose $f = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$. Then $0 = \sigma(0) = \sigma(\alpha_0 + \alpha_1 a + \cdots + \alpha_n a^n) = \alpha_0 + \alpha_1 \sigma(a) + \cdots + \alpha_n \sigma(a)^n$ and thus $\sigma(a)$ is a root of $f$. □
Proposition 2.18 Suppose $f \in \mathbb{K}[X]$ has $n \geq 1$ distinct roots in a splitting field $F$ over $\mathbb{K}$, then $G = \text{Aut}_F \mathbb{K}$ is isomorphic to a subgroup of $S_n$.

Proof. Suppose that the roots are $t_1, t_2, \ldots, t_n$. Let $I = \{t_1, \ldots, t_n\}$. By the last lemma we know that the elements in $G$ permute the $n$ roots. We thus get a homomorphism

$$\Psi : \text{Aut}_F \mathbb{K} \to \text{Sym}(I), \phi \mapsto \phi|_I.$$ 

The map is also injective as $F = \mathbb{K}(t_1, \ldots, t_n)$ and thus every $\sigma \in \text{Aut}_F \mathbb{K}$ is determined by its values in $t_1, \ldots, t_n$. We thus have that $\text{Aut}_F \mathbb{K}$ is isomorphic to $\text{Im} \Psi$ that is a subgroup of $\text{Sym}(I)$. As $|I| = n$ we have that $\text{Sym}(I)$ is isomorphic to $S_n$ and hence the result. $\square$
3 Separability, Normality and Galois Extensions

In this section we will introduce some conditions on field extensions $K \subseteq F$ that will ensure that we get a 1-1 correspondence between the collection of intermediate fields of the extension and the subgroups of the Galois group.

I. Separability.

Definition.

(1) We say that an irreducible polynomial $f$ over $K$ is separable if it has no multiple root in a splitting field over $K$.

(2) An element $a \in F$ is said to be separable over $K$ if it is algebraic over $K$ and its minimal polynomial over $K$ is separable.

(3) An algebraic field extension $K \subseteq F$ is said to be separable if all elements $a \in F$ are separable over $K$.

Remark. Let $F_1$ and $F_2$ be two splitting fields of $f \in K[x]$. By Theorem 2.13 there is a field isomorphism $\phi : F_1 \to F_2$ such that $\phi(a) = a$ for all $a \in K$. Suppose that $f$ has no multiple roots in $F_1$. Thus

$$f = c(x - t_1) \cdots (x - t_n)$$

with $c \in K$ and $t_1, \ldots, t_n$ distinct elements in $F_1$. Then

$$f = \phi^*(f) = c(x - \phi(t_1)) \cdots (x - \phi(t_n)).$$

As $\phi$ is an isomorphism we also have that $\phi(t_1), \ldots, \phi(t_n)$ are distinct. Thus the definition (1) above makes sense as it doesn’t depend on what the splitting field is. No surprise as all the splitting fields are isomorphic.

Examples.

(1) $f = x^2 + x + 1$ is separable over $\mathbb{Q}$. It has the distinct roots $\frac{-1 \pm i\sqrt{3}}{2}$.

(2) Let $K = \mathbb{Z}_2(t)$, the field of rational expressions over $\mathbb{Z}_2$ in the free variable $t$. Consider the polynomial

$$f = x^2 - t \in K[X].$$

(a) $f$ is irreducible over $K$: otherwise $(f/g)^2 = t$ for some polynomials $f, g \in \mathbb{Z}_2[t]$. But then

$$f^2 = tg^2$$
which is absurd as the left hand side is of even degree and the right hand side of odd degree.

(b) We show that $f$ is not separable. Let $F$ be a splitting field of $f$ over $K$ and let $a$ be a root of $f$ in $F$. Then

$$(x - a)^2 = x^2 - a^2 = x^2 - t.$$ 

Thus $a$ is double root of $f$.

**Definition.** (Formal derivation). We introduce a map $D : K[x] \rightarrow K[x]$. For

$$f = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$$

we let

$$D(f) = a_1 + 2a_2 x + \cdots + na_n x^{n-1}.$$ 

We call $D(f)$ the formal derivative of $f$.

**Remark.** Notice that if $K \subseteq F$ and $f \in K[x]$, then the derivative of $f \in K[x]$ is the same as the derivative of $f \in F[x]$.

**Lemma 3.1** Let $f, g \in K[x]$ and $a \in K$.

1. $D(f + g) = D(f) + D(g)$
2. $D(af) = aD(f)$
3. $D(fg) = D(f)g + fD(g)$

**Proof** See Problem Sheet 6.

**Remark.** For some of the results in this section we need to use the following fact. If $0 \neq f, g \in K[x]$ and $K \subseteq F$ then a gcd of $f, g$ in $K[x]$ is also a gcd of $f, g \in F[x]$. To see this, let $d$ be the greatest common divisor of $f, g$ in $K[x]$. If $f = dh$ and $g = dk$ with $h, k \in K[x]$, then $h, k \in F[x]$ as well and thus $d|f$ and $d|g$ in $F[x]$. Now we know that

$$d = af + bg$$

for some $a, b \in K[x]$. It follows from this that if $c$ divides $f, g$ in $F[x]$ then it divides $d$ in $F[x]$. Hence $d$ is a gcd of $f$ and $g$ in $F[x]$.

**Lemma 3.2** Let $f \in K[x]$ be a polynomial of degree at least 1. Then $f$ has no multiple root in a splitting field $F$ if and only if $f$ and $D(f)$ are coprime in $K[x]$.

**Proof** ($\Leftarrow$). We argue by contradiction and suppose $f = (x - a)^2 g$ over $F$. Then, working in $F[x]$,

$$D(f) = 2(x - a)g + (x - a)^2 D(g)$$

and $f$ and $D(f)$ have the common divisor $(x - a)$ and thus can’t be coprime in $F[x]$ and then they can’t be coprime in $K[x]$ either by the remark above. But this contradicts our assumption that $f$ and $g$ were coprime in $K[x]$.
\((\Rightarrow)\). Suppose that \(f = c(x - a_1) \cdots (x - a_n)\) over \(\mathbb{F}\) where \(c \in \mathbb{K}\) and \(a_1, \ldots, a_n\) are distinct elements in \(\mathbb{F}\). Then

\[
D(f) = c \sum_{k=1}^{n} (x - a_1) \cdots (x - a_{k-1})(x - a_{k+1}) \cdots (x - a_n).
\]

We want to show that \(f\) and \(D(f)\) are coprime. The only way this would fail is if they had some common irreducible factor that would then have to be some \((x - a_j)\). However,

\[
D(f)(a_j) = c(a_j - a_1) \cdots (a_j - a_{j-1})(a_j - a_{j+1}) \cdots (a_j - a_n) \neq 0,
\]

which shows that no \((x - a_j)\) is a factor of \(D(f)\) and thus that \(f\) and \(D(f)\) are coprime. \(\Box\)

**Corollary 3.3** An irreducible polynomial \(f \in \mathbb{K}[x]\) is separable if and only if \(D(f) \neq 0\).

**Proof** If \(f\) is irreducible then \(f\) and \(D(f)\) have a common divisor if and only if \(f\) divides \(D(f)\). But as \(D(f)\) is of lower degree than \(f\), this happens if and only if \(D(f) = 0\). \(\Box\)

**Theorem 3.4** Let \(f \in \mathbb{K}[x]\) be irreducible.

(a) If \(\text{char} \mathbb{K} = 0\) then \(f\) is separable.

(b) If \(\text{char} \mathbb{K} = p\) for a prime \(p\), then \(f\) is separable if and only if \(f \not\in \mathbb{K}[x^p]\).

**Proof** (a) Suppose the leading coefficient of \(f\) is \(a_n \neq 0\). Notice that \(n \geq 1\). The leading coefficient of \(D(f)\) is then \(na_n\) that is not zero as \(\text{char} \mathbb{K} = 0\).

(b) We have that

\[
D(a_0 + a_1x + \cdots + a_nx^n) = a_1 + 2a_2x + \cdots + na_nx^{n-1}
\]

is zero iff \(a_n = 0\) for all \(n\) that are coprime to \(p\) iff the polynomial is in \(\mathbb{K}[x^p]\). \(\Box\)

**Corollary 3.5** Let \(\mathbb{K} \subseteq \mathbb{F}\) be an algebraic field extension where \(\text{char} \mathbb{K} = 0\). Then \(\mathbb{K} \subseteq \mathbb{F}\) is separable.

**Proof** Let \(a \in \mathbb{F}\). The minimal polynomial \(f\) of \(a\) over \(\mathbb{K}\) is irreducible and by Theorem 3.4 it is thus separable. Hence \(a\) is separable over \(\mathbb{K}\). \(\Box\)

**Remark.** Let \(\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{F}\) be an ascending chain of fields where \(\mathbb{K} \subseteq \mathbb{F}\) is separable. Then both \(\mathbb{K} \subseteq \mathbb{M}\) and \(\mathbb{M} \subseteq \mathbb{F}\) are separable. To see that \(\mathbb{K} \subseteq \mathbb{M}\) is separable let \(a \in \mathbb{M}\). As \(a \in \mathbb{F}\) we know that \(a\) is separable over \(\mathbb{K}\). To see that \(\mathbb{M} \subseteq \mathbb{F}\) is separable let \(a \in \mathbb{F}\). The minimal polynomial \(m_{\mathbb{K}}\) of \(a\) in \(\mathbb{K}[x]\) is a polynomial in \(\mathbb{M}[x]\) that maps \(a\) to zero and thus it must be divisible by the minimal polynomial \(m_{\mathbb{M}}\) of \(a\) in \(\mathbb{M}[x]\). As \(m_{\mathbb{K}}\) is separable the same is true its divisor \(m_{\mathbb{M}}\).

**Remark.** Let \(f, g \in \mathbb{K}[x]\) and suppose \(\mathbb{K} \subseteq \mathbb{F}\). Recall from earlier that if \(d\) is a gcd of \(f, g\) in \(\mathbb{K}[x]\) then \(d\) is also a gcd of \(f, g\) in \(\mathbb{F}[x]\). In particular if \(d\) is the unique monic gcd of \(g, f\) in \(\mathbb{K}[x]\) then \(d\) is also the unique monic gcd of \(g, f\) in \(\mathbb{F}[x]\). This fact will be important in the proof of the following result.
Theorem 3.6 Let $K \subseteq F$ be a finite extension where either

(a) $K$ is finite

or

(b) $K$ is infinite and $K \subseteq F$ is separable.

Then $F = K(\theta)$ for some $\theta \in F$.

Proof Suppose first that $K$ is a finite field. Then $F$ is also finite and we know from Group Theory (http://people.bath.ac.uk/gt223/MA30237.html, Sheet 5: Question 5) that the group of units $F^* = F \setminus \{0\}$ is a cyclic group, say generated by $\theta$. Thus $F = K(\theta)$.

We can thus assume that $K$ is an infinite field. Notice that $K \subseteq F$ is finitely generated and arguing by induction, it is sufficient to prove this in the case when there are two generators, say $F = K(\alpha, \beta)$. Let $f, g$ be the minimal polynomials of $\alpha, \beta$ over $K$. Take a splitting field $L$ of $fg$ over $F$. Suppose

$$f = (x - \alpha_1) \cdots (x - \alpha_n)$$
$$g = (x - \beta_1) \cdots (x - \beta_m),$$

where $\alpha = \alpha_1, \ldots, \alpha_n \in L$ are distinct (as the extension is separable) and likewise $\beta = \beta_1, \ldots, \beta_m \in L$ are distinct. Let

$$\theta = \alpha + c\beta$$

where $c \in K$ will be specified later. Let

$$h = f(x - \theta) \in K(\theta)[x].$$

Notice that $h(\beta) = f(\theta - c\beta) = f(\alpha) = 0$ and thus $x - \beta$ is a common irreducible factor of $h, g$. The aim is to show that one is able to pick $c \in K$ such that the unique gcd of $h, g$ in $L[x]$ is $x - \beta$ (and therefore by the remarks also the unique gcd of $h, g$ in $K(\theta)[x]$ where both $g, h$ are). This is going to be the case iff none of the factors $x - \beta_2, \ldots, x - \beta_m$ of $g$ are factors of $h$ that happens iff none of $\beta_2, \ldots, \beta_m$ is a root of $h$. To see what could go wrong notice that for $2 \leq j \leq m$,

$$h(\beta_j) = 0 \iff f(\theta - c\beta_j) = 0 \iff \theta - c\beta_j = \alpha_i \text{ for some } 1 \leq i \leq n
\iff \alpha + c\beta - c\beta_j = \alpha_i \text{ for some } 1 \leq i \leq n
\iff c = \frac{\alpha_i - \alpha}{\beta - \beta_j} \text{ for some } 1 \leq i \leq n.$$

(Notice that the denominator is nonzero as $\beta \neq \beta_j$ that we know is the case as the extension in separable). As there are only finitely many expressions of the form $(\alpha_i - \alpha)/(\beta - \beta_j)$, with $1 \leq i \leq n$ and $2 \leq j \leq m$, and as $K$ is infinite, we can choose $c \in K$ so that it is different from all of these expressions. As we have pointed out above this then implies that none of $\beta_2, \ldots, \beta_m$ is a root of $h$ and hence the unique monic gcd of $h, g$ in $L[x]$ is $x - \beta$. This is however also the unique monic gcd of $h, g$ in $K(\theta)[x]$. In particular $x - \beta \in K(\theta)[x]$ and thus $\beta \in K(\theta)$. Then also $\alpha = \theta - c\beta \in K(\theta)$ and we have shown that $F = K(\alpha, \beta) = K(\theta)$. □
II. Normality

**Definition.** An algebraic field extension $K \subseteq F$ is said to be normal if, for all $a$ in $F$, the minimal polynomial of $a$ over $K$ splits into linear factors over $F$.

**Remark.** Equivalently $K \subseteq F$ is normal if whenever $f \in K[x]$ is irreducible over $K$ with a root in $F$, then all the roots of $f$ must be in $F$.

**Examples.** (1) $\mathbb{R} \subseteq \mathbb{C}$ is normal.

(2) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ is not normal as $\sqrt{2}$ is the only real root of $x^2 - 2$.

**Lemma 3.7** Let $K \subseteq M \subseteq F$ be an ascending chain of fields where $K \subseteq F$ is normal. Then $M \subseteq F$ is normal.

**Proof** Let $a \in F$ and let $f_K, f_M$ be the minimal polynomials of $a$ over $K, M$. As $K \subseteq F$ is normal we know that $f_K$ splits into linear factors over $F$, say

$$f_K = (x - a_1) \cdots (x - a_n)$$

where $a = a_1, a_2, \ldots, a_n \in F$. As $f_K(a) = 0$ and $f_K \in M[x]$ it follows that $f_M | f_K$ and thus $f_M$ also splits into a product of linear factors over $F$. $\square$

**Remarks.** (1) In general if $K \subseteq M, M \subseteq F$ are normal it does not follow that $K \subseteq F$ is normal. For example $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{3})$ are normal as they are of degree 2 (see Problem Sheet 6). However $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ is not normal. The element $\sqrt{2}$ has minimal polynomial $x^2 - 2$ over $\mathbb{Q}$ but only two of the roots are in $\mathbb{Q}(\sqrt{2})$ (in fact only two roots are real) namely $\pm \sqrt{2}$.

(2) Let $K \subseteq M \subseteq F$ be an ascending chain of fields where $K \subseteq F$ is normal. In general it does not follow that $K \subseteq M$ is normal. Consider for example $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{A}$ where $\mathbb{A} = \mathbb{A}_{\mathbb{C}/\mathbb{Q}}$ is the field of the algebraic elements in $\mathbb{C}$ over $\mathbb{Q}$. Here $\mathbb{Q} \subseteq \mathbb{A}$ is normal but $\mathbb{Q} \not\subseteq \mathbb{Q}(\sqrt{2})$ is not normal.

**Remark.** Let $F$ be a splitting field of some $f \in K[x]$ over $K$, say $F = K(a_1, \ldots, a_n)$ where $a_1, \ldots, a_n \in F$ are the roots of $f$ in $F$. If $F \subseteq F(b)$ is any field extension then $F(b)$ is a splitting field of $f$ over $K(b)$. This is because $F(b) = K(b, a_1, a_2, \ldots, a_n)$ and $a_1, \ldots, a_n$ are the roots of $f$ (that is also in $K(b)[x]$). We will make use of this observation in the proof of the following theorem.

**Theorem 3.8** The field extension $K \subseteq F$ is normal and finite if and only if $F$ is a splitting field of some polynomial $f \in K[x]$ over $K$.

**Proof** ($\Rightarrow$). Suppose $F = K(a_1, a_2, \ldots, a_n)$ and let $f_i$ be the minimal polynomial of $a_i$ over $K$. Then let

$$f = f_1 \cdots f_n.$$ 

The roots of $f$ are $a_1, a_2, \ldots, a_n$ and some extra roots $b_1, \ldots, b_m$ that are also in $F$ as $K \subseteq F$ is normal. Thus

$$F = K(a_1, \ldots, a_n, b_1, \ldots, b_m).$$

27
and thus a splitting field of \( f \) over \( K \).

(\( \Leftarrow \)). Suppose \( F \) a splitting field of \( f \in K[x] \) over \( K \). The extension \( K \subseteq F \) is clearly finite as it is generated by finitely many algebraic elements over \( K \) (see Theorem 2.9) and it remains to see that it is normal.

Let \( g \in K[x] \) be an irreducible polynomial with a root \( \theta_1 \in F \) and let \( \theta_2 \) be any root of \( g \) in a splitting field \( L \) of \( g \) over \( F \). We want to show that \( \theta_2 \in F \). First notice that \( K(\theta_1) \cong K[x]/K[x]g \cong K(\theta_2) \) as \( \theta_1, \theta_2 \) have the same minimal polynomial \( g \) over \( K \). Let \( \phi : K(\theta_1) \rightarrow K(\theta_2) \) be an isomorphism between the two fields. As \( F(\theta_2) \) is the splitting field of \( f \) over \( K(\theta_2) \) we can apply Theorem 2.13 that tells us that there is a field isomorphism \( \psi : F(\theta_1) \rightarrow F(\theta_2) \)

such that \( \psi|_{K(\theta_1)} = \phi \). From Exercise 1 on Sheet 3 we know that \( [F(\theta_1) : K(\theta_1)] = [\psi(F(\theta_1)) : \psi(K(\theta_1))] = [F(\theta_2) : K(\theta_2)] \). From this and \( [K(\theta_1) : K] = \deg g = [K(\theta_2) : K] \), we get from the Tower Law that

\[
[F(\theta_1) : K] = [F(\theta_1) : K(\theta_1)][K(\theta_1) : K] = [F(\theta_2) : K(\theta_2)][K(\theta_2) : K] = [F(\theta_2) : K].
\]

A second application of the tower law gives then

\[
[F(\theta_1) : F][F : K] = [F(\theta_2) : F][F : K]
\]

from which we deduce that \( [F(\theta_2) : F] = [F(\theta_1) : F] = 1 \) (as \( \theta_1 \in F \)) and therefore that \( \theta_2 \in F \). This finishes the proof. \( \square \)

III. Galois extensions

Let \( K \subseteq F \) be a finite field extension. We have seen on Problem Sheet 3 that in the case when the extension is not separable or not normal then the Galois Correspondence between intermediate subfields of \( K \subseteq F \) and subgroups of the Galois Group can fail to be 1-1. We will see in next chapter that if we add the constraints that the extension is both normal and separable then the Galois Correspondence turns out to be bijective providing some close interplay between the Galois Group and the field extension. We will end this chapter by characterising such extensions in terms of splitting fields. We start with a lemma that will be useful in understanding the size of the Galois Group of a given field extension (see the corollary to the lemma). The Lemma is given in a bit more general form as this will be needed later.

**Lemma 3.9** Let \( K_1 \subseteq F_1 \) and \( K_2 \subseteq F_2 \) be finite extensions where \( [F_1 : K_1] = [F_2 : K_2] \). Let \( \phi : K_1 \rightarrow K_2 \) be a field isomorphism. Then there are at most \( [F_1 : K_1] \) field isomorphisms \( \psi : F_1 \rightarrow F_2 \) that extend \( \phi \), that is such that \( \psi|_{K_1} = \phi \).

**Proof** We prove this by induction on \( [F_1 : K_1] \). When \( [F_1 : K_1] = 1 \) then \( F_1 = K_1 \), \( F_2 = K_2 \) and \( \psi = \phi \) is clearly then only isomorphism extending \( \phi \). Now suppose \( [F_1 : K_1] > 1 \) and that the result holds whenever the degree is smaller. Let \( a \in F_1 \setminus K_1 \) and
let $f \in \mathbb{K}_1[x]$ be its minimal polynomial over $\mathbb{K}$. If $\psi : F_1 \to F_2$ extends $\phi$ then we know from Lemma 2.16 that $b = \psi(a)$ must be a root of $\phi^*(f)$ in $F_2$. In which case $\psi$ induces an isomorphism $\phi_b : \mathbb{K}_1(a) \to \mathbb{K}_2(b)$ such that $\phi_b(a) = b$ and $\phi_b|_{\mathbb{K}_1} = \phi$. There are at most $\deg f = [\mathbb{K}_2(a) : \mathbb{K}_2] = [\mathbb{K}_1(a) : \mathbb{K}_1]$ such roots $b$ of $\phi^*(f)$ (see Proposition 2.6) and by induction hypothesis each such $\phi_b$ has then at most $[F_1 : \mathbb{K}_1(a)]$ extensions $\tau : F_1 \to F_2$. Thus in total we get at most

$$[\mathbb{K}_1(a) : \mathbb{K}_1][F_1 : \mathbb{K}_1(a)] = [F_1 : \mathbb{K}_1]$$

extensions of $\phi$. This finishes the proof. $\square$

**Corollary 3.10** If $\mathbb{K} \subseteq F$ is any finite field extension, then $|\text{Aut}_F \mathbb{K}| \leq [F : \mathbb{K}]$.

**Proof** Take $\mathbb{K}_1 = \mathbb{K}_2$, $F_1 = F_2$ and $\phi = \text{id}$ in Lemma 3.9. $\square$.

**Remark.** We will see that when we add normality and separability we will get equality in the last result. This is essentially going to follow from next proposition. We have defined earlier what we mean by an irreducible polynomial to be separable. We now extend the definition.

**Definition.** A polynomial $f \in \mathbb{K}[x]$ is separable if none of its irreducible factors over $\mathbb{K}$ have a multiple root.

**Remark.** Notice that we only require the irreducible factors to have no multiple roots. For example we have that $(x - 1)^2 \in \mathbb{Z}_2[x]$ is separable over $\mathbb{Z}_2$. Although $f$ has a multiple root, its irreducible factors do not have a multiple root. Notice also that we know that all polynomials in $\mathbb{K}[x]$ are separable when $\text{char} \mathbb{K} = 0$. This follows from Theorem 3.4.

**Proposition 3.11** Let $\phi : \mathbb{K}_1 \to \mathbb{K}_2$ be a field isomorphism and let $f \in \mathbb{K}_1[x]$ be a separable polynomial of degree at least one. Let $F_1$ be a splitting field of $f$ over $\mathbb{K}_1$ and let $F_2$ be a splitting field of $\phi^*(f)$ over $\mathbb{K}_2$. Then there are exactly $[F_1 : \mathbb{K}_1]$ isomorphisms $\psi : F_1 \to F_2$ that extend $\phi$.

**Proof** We prove this by induction on $[F_1 : \mathbb{K}_1]$. Suppose first that $[F_1 : \mathbb{K}_1] = 1$. Then $f$ splits into linear factors over $\mathbb{K}_1$, say

$$f = c(x - a_1) \cdots (x - a_n)$$

with $c, a_1, \ldots, a_n \in \mathbb{K}_1$. Hence $\phi^*(f) = \phi(c)(x - \phi(a_1)) \cdots (x - \phi(a_n))$ and $\phi^*(f)$ also splits over $\mathbb{K}_2$. Hence $F_2 = \mathbb{K}_2$ and $\psi = \phi$ is clearly the unique extension of $\phi$.

Now suppose that $[F_1 : \mathbb{K}_1] > 1$ and that the result holds whenever the degree is smaller. As $F_1 \neq \mathbb{K}_1$, $f$ must have an irreducible factor $g$ of degree at least 2. Let $a$ be any root of $g$ in $F_1$. Let $b$ be any root of $\phi^*(g)$ (that is then an irreducible factor of $\phi^* (f)$) in $F_2$. By Lemma 2.12 there exists a field isomorphism $\phi_b : \mathbb{K}_1(a) \to \mathbb{K}_2(b)$ that maps $a$ to $b$ and where $\phi_b|_{\mathbb{K}_1} = \phi$. As $f$ (and thus $\phi^*(f)$) is separable we have that there are exactly $\deg g = [\mathbb{K}_1(a) : \mathbb{K}_1]$ roots $b$ of $\phi^*(g)$ (see Proposition 2.6). Now observe that $F_1$ is the splitting field of $f$ over $\mathbb{K}_1(a)$ and that $F_2$ is the splitting field of $\phi_b^*(f) = \phi^*(f)$ over
Theorem 3.13
Let $K$. Thus by induction hypothesis, there are for each root $b$ exactly $[F_1 : K_1(a)]$ field isomorphisms $\psi : F_1 \to F_2$ that extend $\phi_b$. As there are $[K_1(a) : K_1]$ such roots we get in total at least

$$[F_1 : K_1(a)][K_1(a) : K_1] = [F_1 : K_1]$$

extensions of $\phi$. From Lemma 3.9 we know that there are at most $[F_1 : K_1]$ of these. Hence we get the equality. \(\square\)

**Remark.** Taking $K_1 = K_2 = K$, $F_1 = F_2 = F$ and $\phi = \text{id}$ we get in particular that if $F$ is the splitting field of a separable polynomial $f \in K[x]$, of degree at least 1, then $|\text{Aut}_KF| = [F : K]$.

**Theorem 3.12** Let $K \subseteq F$ be a field extension. The following are equivalent.

(a) $K \subseteq F$ is finite, normal and separable.
(b) $F$ is a splitting field of some separable polynomial $f \in K[x]$ of degree at least 1.

**Proof** (a)\(\Rightarrow\) (b). By Theorem 3.8 we know that $F$ is a splitting field of some polynomial $f \in K[x]$ of degree at least 1. To see that $f$ is separable we need to show that none of its irreducible factors over $K$ have multiple root. Let $g$ thus be one of the irreducible factors and let $a$ be one of the roots. Then $g$ is the minimal polynomial of $a$ over $K$ and as the extension is separable we know that $g$ has no multiple root.

(b)\(\Rightarrow\)(a). From Theorem 3.8 we know that the extension is finite and normal. We argue by contradiction and suppose that there is an element $a \in F$ whose minimal polynomial $g$ has a multiple root $a$. Let $\psi \in \text{Aut}_KF$ and consider the induced field isomorphism $\phi : K(a) \to \psi(K(a))$, $t \mapsto \psi(t)$. We know from Corollary 2.17 that $b = \psi(a)$ is another root of $g$ and then $\psi(K(a)) = K(b)$ and $\phi = \phi_b : K(a) \to K(b)$ where $\phi_b(a) = b$ and $\phi_b(t) = t$ for all $t \in K$. As $g$ has multiple roots we get less than $\deg g = [K(a) : K]$ elements $\psi \in \text{Aut}_KF$ that extend $\phi_b$. Thus we have less than

$$[F : K(a)] \cdot \deg g = [F : K(a)] \cdot [K(a) : K] = [F : K]$$

elements in $\text{Aut}_KF$. This contradicts however Proposition 3.11 (see the remark after it). \(\square\)

**Definition.** We say that a field extension $K \subseteq F$ is a *Galois extension* if it satisfies the following equivalent conditions.

(a) $K \subseteq F$ is finite, normal and separable.
(b) $F$ is the splitting field of some separable $f \in K[x]$, of degree at least 1, over $K$.

The following will be one of the main ingredients for the Fundamental Theorem of Galois Theory.

**Theorem 3.13** Let $K \subseteq F$ be a Galois extension. Then

(a) $|\text{Aut}_KF| = [F : K]$.
(b) For any $K \subseteq M \subseteq F$ and any $\phi \in \text{Aut}_KM$, there exists $\psi \in \text{Aut}_KF$ such that $\psi|_M = \phi$. 

30
Proof Part (a) we have already dealt with (see the remark after Proposition 3.11). The part (b) is also a consequence of Proposition 3.11 (see sheet 7 for the details).
I. The Fundamental Theorem

Throughout this section $K \subseteq F$ will be a Galois extension.

**Proposition 4.1** Let $H$ a subgroup of $G = \text{Aut}_KF$. Then $[F : \text{Fix}H] = |H|$.

**Proof.** By Theorem 3.6 we know that the extension $K \subseteq F$ is simple, say $F = K(a)$. Let $B = \{\sigma(a) : \sigma \in H\}$. Notice that $\tau H = H$ for all $\tau \in H$ and therefore $\tau(B) = B$. Now consider the polynomial $f = \prod_{b \in B} (X - b)$. As $\tau(B) = B$, we have

$$\tau^*(f) = \prod_{b \in B} (x - \tau(b)) = \prod_{c \in \tau(B)} (x - c) = \prod_{c \in B} (x - c) = f.$$ 

Thus all the coefficients of $f$ are in $M = \text{Fix}H$ and $f$ is a polynomial over $M$. Notice also that $f$ must be irreducible over $M$. To see this argue by contradiction and suppose that $f = gh$ with $g, h \in M[x]$ both of degree less than $\text{deg}f$. Without loss of generality we can suppose that $a$ is a root of $g$. Notice that as all the elements of $H$ fix the elements in $M = \text{Fix}H$ pointwise we have that $\tau^*(g) = g$ for all $\tau \in H$. But this implies that $\tau(a)$ is a root of $\tau^*(g) = g$ for all $\tau \in H$ and thus all the elements in $B$ (that is all the roots of $f$) are roots of $g$. But this gives us the contradiction that $g = f$. Thus $f$ is irreducible over $M$ and is thus the minimal polynomial of $a$ over $M$. It follows that (see Proposition 2.6)

$$[F : M] = [M(a) : M] = \text{deg}f = |B| \leq |H|.$$ 

On the other hand we know from Lemma 2.5 that $H \leq \Phi \Psi(H)$ and as $M = \Psi(H) \leq F$ is a Galois extension we know from Theorem 3.13 (see Qn1(b) on Sheet 7 for the details) that

$$|H| \leq |\Phi(\Psi(H))| = [F : M].$$

Hence $[F : \text{Fix}H] = |H|$. □

**Lemma 4.2** Let $\sigma \in G = \text{Aut}_KF$ and let $M$ be a field such that $K \subseteq M \subseteq F$. Then

$$\text{Aut}_{\sigma(M)}F = \sigma \cdot \text{Aut}_MF \cdot \sigma^{-1}.$$ 

**Proof** We have that $\tau \in G$ fixes the elements in $\sigma(M)$ pointwise if and only if $\tau \sigma(a) = \sigma(a)$ for all $a \in M$ if and only if $\sigma^{-1} \tau \sigma(a) = a$ for all $a \in M$. But this happens if and only if $\sigma^{-1} \tau \sigma \in \text{Aut}_MF$ that is if and only if $\tau$ is in $\sigma \cdot \text{Aut}_MF \cdot \sigma^{-1}$. □
We are now ready for the main result of this course. Let us first recall the Galois Correspondence. Let
\[ \mathcal{F} = \{ M : K \leq M \leq F \} \], and \( \mathcal{G} = \{ H : H \leq G = \text{Aut}_KF \} \).

We consider the maps
\[ \Phi : \mathcal{F} \to \mathcal{G}, M \mapsto \text{Aut}_MF \]
and
\[ \Psi : \mathcal{G} \to \mathcal{F}, H \mapsto \text{Fix}(H) \].

**Theorem 4.3** (The Fundamental Theorem of Galois Theory). Let \( K \subseteq F \) be a Galois extension with Galois group \( G = \text{Aut}_KF \). Then

1. \( |G| = [F : K] \).
2. \( \Phi \) and \( \Psi \) are mutual inverses and order reversing.
3. If \( M \in \mathcal{F} \) then
   \[ [F : M] = |
   \Phi(M)| \text{ and } [M : K] = |G|/|
   \Phi(M)|. \]
4. For \( M \in \mathcal{F} \), we have that \( K \subseteq M \) is normal if and only if \( \Phi(M) \) is a normal subgroup of \( G \) and then the Galois group of \( K \subseteq M \) is isomorphic to \( G/\Phi(M) \).

**Proof**

(1) This is Theorem 3.13(a).

(2) That the maps are order reversing follows from Lemma 2.5. Let \( M \in \mathcal{F} \). By Theorem 3.13 (see Qn1(b) on Sheet 7 for the details) we have
\[ [F : M] = |\Phi(M)| \text{ and } [F : \Psi\Phi(M)] = |\Phi\Psi\Phi(M)|. \]
By Lemma 2.5, \( \Phi = \Phi\Psi\Phi \) and thus it follows that \( [F : M] = [F : \Psi\Phi(M)] \). By Lemma 2.5 again \( M \leq \Psi\Phi(M) \) and thus we conclude that \( \Psi\Phi(M) = M \). We have thus shown that \( \Psi\Phi = \text{id}_\mathcal{F} \).

Let \( H \in \mathcal{G} \). From Proposition 4.1, we know that
\[ [F : \Psi(H)] = |H| \text{ and } [F : \Psi\Phi\Psi(H)] = |\Phi\Psi(H)|. \]
By Lemma 2.5 we have \( \Psi = \Psi\Phi\Psi \) and thus it follows that \( |\Phi\Psi(H)| = |H| \). From Lemma 2.5 again we know that \( H \leq \Phi\Psi(H) \) and thus we conclude that \( \Phi\Psi(H) = H \). We have thus shown that \( \Phi\Psi = \text{id}_\mathcal{G} \).

(3) We have already established the first identity. For the latter simply observe that
\[ [M : K] = \frac{[F : K]}{[F : M]} = |G|/|\Phi(M)|. \]

(4) We first show that \( K \subseteq M \) is normal if and only if \( \sigma(M) = M \) for all \( \sigma \in G = \text{Aut}_KF \). First suppose that \( K \subseteq M \) is normal and let \( \sigma \in G \). For any \( a \in M \) we have that the \( \sigma(a) \) must be a root of the minimal polynomial of \( a \) over \( K \) (see Corollary 2.17). As \( K \subseteq M \) is normal we know however that all the roots are in \( M \). Hence \( \sigma(a) \in M \). This shows that \( \sigma(M) \subseteq M \). Then also \( \sigma^{-1}(M) \subseteq M \) and thus \( M = \sigma\sigma^{-1}(M) \subseteq \sigma(M) \). We have thus \( \sigma(M) = M \) for all \( \sigma \in G \). Conversely suppose that \( \sigma(M) = M \) for all \( \sigma \in G \). Let \( a \in M \).
and let \( f \in \mathbb{K}[x] \) be the minimal polynomial of \( a \) over \( \mathbb{K} \). Let \( b \) be any other root of \( f \) in \( \mathbb{F} \) we want to show that \( b \in \mathbb{M} \). By Lemma 2.12 we know that there is a field isomorphism \( \phi_b : \mathbb{K}(a) \to \mathbb{K}(b) \) that maps \( a \) to \( b \) and fixes \( \mathbb{K} \) pointwise. By Proposition 3.11 we can extend \( \phi_b \) to an element \( \tau \in G \) (that is such that \( \tau|_{\mathbb{K}(a)} = \phi_b \). But by our assumption we know that \( \tau(\mathbb{M}) = \mathbb{M} \) and hence in particular \( b = \tau(a) \in \mathbb{M} \). We have thus established our claim.

To finish the proof of (4) we use Lemma 4.2. We have that \( \mathbb{K} \subseteq \mathbb{M} \) is normal if and only if \( \sigma(\mathbb{M}) = \mathbb{M} \) for all \( \sigma \in G \). But by our assumption we know that \( \tau(\mathbb{M}) = \mathbb{M} \) and hence in particular \( b = \tau(a) \in \mathbb{M} \). We have thus established our claim.

II. Examples

We will consider two general examples that are both interesting for us with respect to the general theory. The first deals with finite fields and the 2nd with the roots of unity in fields of characteristic 0.

A. Finite fields.

We have seen that for each prime \( p \) and each positive integer \( n \) there is (up to isomorphism) exactly one finite field of order \( p^n \) that consists of the roots of \( x^{p^n} - x \) in a splitting field over \( \mathbb{Z}_p \) (and thus is itself the splitting field). Notice that the there are no multiple roots of \( x^{p^n} - x \) and thus it is separable. We thus have that \( \mathbb{Z}_p \subseteq \mathbb{F} \) is a Galois extension and we can apply the Fundamental Theorem of Galois Theory.

**Theorem 4.4** Let \( \mathbb{F} \) be a field of order \( p^n \). Then the Galois group of \( \mathbb{Z}_p \subseteq \mathbb{F} \) is cyclic of order \( n \).

**Proof** Let \( G \) be the Galois group. By the Fundamental Theorem of Galois Theory we know that \( |G| = [\mathbb{F} : \mathbb{Z}_p] = n \). Consider the map \( \phi : \mathbb{F} \to \mathbb{F} \), \( a \mapsto a^p \). We have that if \( \phi(a) = \phi(b) \) then \( 0 = \phi(a) - \phi(b) = a^p - b^p = (a - b)^p \) (where the last identity holds as the characteristic is \( p \)) and thus \( a = b \). This shows that \( \phi \) injective and as \( \mathbb{F} \) is finite, \( \phi \) is then a bijection. Also \( \phi(1) = 1 \), \( \phi(ab) = (ab)^p = a^p b^p \) and \( \phi(a + b) = (a + b)^p = a^p + b^p \). We thus have \( \phi \) is an automorphism and by the little Fermats Theorem we also know that \( \phi(a) = a^p = a \) for all \( a \in \mathbb{Z}_p \). Thus \( \phi \) is in the Galois group \( G = \text{Aut}_{\mathbb{Z}_p} \mathbb{F} \). In order to
Now consider where \( t \phi \) is the number of roots of \( x^{p^n} - x \) that is absurd as \( p^n > p^m \). This finishes the proof. \( \square \)

Remark. We know from Group Theory that for each divisor \( d \) of \( n \) there is exactly one subgroup of this order. Notice how this matches the situation with the field \( \bar{F} \) (see Exercise 5 on Sheet 5) where we have seen that for each divisor \( d \) of \( n \) there exists exactly one subfield of order \( p^d \).

**Theorem 4.5** We have that \( x^{p^n} - x \in \mathbb{Z}_p[x] \) is the product of all the monic irreducible polynomials over \( \mathbb{Z}_p \) whose degree divide \( n \).

**Proof** Let \( \mathbb{F} \) be the roots of of \( x^{p^n} - x \) in a splitting field (and thus \( \mathbb{F} \) the splitting field). Let \( f \) be any irreducible monic factor of \( x^{p^n} - x \) and let \( a \) be any root of \( f \) in a \( \mathbb{F} \). Then

\[ n = [\mathbb{F} : \mathbb{Z}_p] = [\mathbb{F} : \mathbb{Z}_p[a]] \cdot [\mathbb{Z}_p[a] : \mathbb{Z}_p] = [\mathbb{F} : \mathbb{Z}_p[a]] \cdot \deg f \]

and thus \( \deg f \) divides \( n \). Conversely let \( f \) be any irreducible polynomial over \( \mathbb{Z}_p \) of degree \( d \) where \( d \mid n \). Consider the field \( \mathbb{Z}_p[x]/\mathbb{Z}_p[x]f = \mathbb{Z}_p[t] \) where \( f \) is a the minimal polynomial of \( t \) over \( \mathbb{Z}_p \). As \( \mathbb{K} = \mathbb{Z}_p[t] \) is a field of order \( p^d \) we know (Exercise 5 on Sheet 5) that \( \mathbb{F} \) has a copy of \( \mathbb{K} \) as subfield and thus \( t \) is root of \( x^{p^n} - x \). As \( f \) is the minimal polynomial of \( t \) it follows that \( f \mid (x^{p^n} - x) \). \( \square \)

**B. The polynomial \( x^n - 1 \in \mathbb{Q}[x] \).**

Let \( \mathbb{F} \) be a splitting field of \( x^n - 1 \) over \( \mathbb{Q} \). From Group Theory we know that the roots form a cyclic multiplicative subgroup of \( \mathbb{F} \setminus \{0\} \), say \( \langle w \rangle \) (as it is a finite subgroup of a field). This can also be seen from the fact that all the roots in \( \mathbb{C} \) can be generated by \( w = e^{2\pi i/n} \).

Notice that \( w^k, \ 1 \leq k \leq n \), has order \( n \) if and only if \( k \) is coprime to \( n \) and thus the number of roots of \( x^n - 1 \) that have order \( n \) (that is the primitive \( n \)th roots of unity) is \( \phi(n) \) where \( \phi \) is the Euler function. Now let

\[ \Phi_n(x) = (x - t_1) \cdots (x - t_{\phi(n)}) \]

where \( t_1, \ldots, t_{\phi(n)} \) are the primitive \( n \)th roots of unity. This gives us a polynomial of degree \( \phi(n) \). Now every root of \( x^n - 1 \) has order \( d \) dividing \( n \) and thus

\[ x^n - 1 = \prod_{d \mid n} \Phi_d(x). \tag{1} \]

Now consider \( x^n - 1 \) as a polynomial in \( \mathbb{Z}[x] \). If we know all the \( \Phi_d \) for \( d < n \) and \( d \mid n \) then we can use (1) to determine \( \Phi_n \) by dividing \( x^n - 1 \) by the product of all the \( \Phi_d \) with \( d < n, d \mid n \). This gives us recursively that \( \Phi_n \) is a monic polynomial in \( \mathbb{Z}[x] \) (See problem sheet 8). In fact it turns out that \( \Phi_n \) is irreducible over \( \mathbb{Q} \).

**Theorem 4.6** The polynomial \( \Phi_n \) is irreducible over \( \mathbb{Q} \).
Proof. Let $w$ be a primitive $n$th root of unity in a splitting field of $F$ of $x^n - 1$ over $\mathbb{Q}$ and let $f$ be the minimal polynomial of $w$ over $\mathbb{Q}$. As $f$ is monic and divides $x^n - 1$ we have in fact that $f \in \mathbb{Z}[x]$ (see sheet 8). The aim is to show that $f = \Phi_n$. We know that $f|\Phi_n$ as $\Phi_n(w) = 0$. In order to show that $f = \Phi_n$ it thus remains to see that all the roots of $\Phi_n$ are roots of $f$. Now let $w^k$ be any of the roots of $\Phi_n$. Thus $1 \leq k \leq n$ and $k$ is coprime to $n$. Suppose $k = p_1 \cdots p_r$ is the prime factorisation of $k$. As $k$ and $n$ are coprime it follows that none of the primes $p_1, \ldots, p_r$ divide $n$. The claim that $w^k = w^{p_1 \cdots p_r}$ is a root of $f$ will thus follow from the following claim.

Claim. If $\theta$ is a root of $f$ and $p$ is a prime that does not divide $n$ then $\theta^p$ is also a root of $f$.

To prove the claim we argue by contradiction and suppose there is a prime $p$ where $p$ does not divide $n$ and were $f(\theta) = 0$ whereas $f(\theta^p) \neq 0$. As $f$ is the minimal polynomial of $w$ it must divide $x^n - 1$ in $\mathbb{Q}[x]$, say

$$x^n - 1 = fg$$

(2)

with $g \in \mathbb{Q}[x]$. In fact $g \in \mathbb{Z}[x]$ (again as $g$ is monic and divides $x^n - 1$). But then $f(\theta^p)g(\theta^p) = (\theta^p)^n - 1 = 0$ and thus $g(\theta^p) = 0$ and $\theta$ is a root of the polynomial $g(x^p)$.

Thus $f|g(x^p)$). Consider the ring homomorphism $\phi_p : \mathbb{Z} \to \mathbb{Z}_p$, $a \mapsto \bar{a}$. For each polynomial $e \in \mathbb{Z}[x]$ we let $\bar{e} = \phi^*(e)$ be the corresponding polynomial in $\mathbb{Z}_p[x]$. By Fermat’s little Theorem we have $\bar{g}[x]^p = \bar{g}[x^p]$. Let $\bar{k}[x]$ be any irreducible factor of $\bar{f}$. As $f|g(x^p)$ we have that $\bar{k}$ then divides $\bar{g}[x]^p = \bar{g}^p$ and thus (as $\bar{k}$ is irreducible) $\bar{k}|\bar{g}$. Thus $\bar{k}$ divides both $\bar{f}$ and $\bar{g}$ and thus $\bar{k}^2$ divides

$$\bar{f}\bar{g} = x^n - 1 \in \mathbb{Z}_p[x]$$

But then we have that $x^n - 1 \in \mathbb{Z}_p[x]$ has a multiple root. For this to be the case we would (by Theorem 3.2) need $x^n - 1$ and $D(x^n - 1) = nx^n - 1$ to have a common irreducible factor. But this is absurd as the only irreducible factor of $D(x^n - 1) = nx^n - 1$ is $x$ that does not divide $x^n - 1$. (Notice that as $p \not| n$ we have that $nx^n \neq 0$). This contradiction finishes the proof of the claim and thus of the Theorem. $\square$

Remark. It follows in particular that $\Phi_n$ is the minimal polynomial of $w$ over $\mathbb{Q}$. 

36
5 Algebraically closed fields and The Fundamental Theorem of Algebra

In this chapter all fields will be of characteristic zero.

Definition. A field $\mathbb{K}$ is algebraically closed if every polynomial in $\mathbb{K}[x]$, of degree at least 1, has a root in $\mathbb{K}$.

Remark. Suppose $\mathbb{K}$ is algebraically closed and that $f \in \mathbb{K}[x]$ has degree at least 1. Then $f$ has a root say $a_1 \in \mathbb{K}$ and thus $f = (x-a_1)g$ for some $g \in \mathbb{K}[x]$. If $g$ has degree at least 1 we can continue and find a root $a_2$ of $g$ in $\mathbb{K}$. Continuing in this manner we see that $f$ splits into linear factors over $\mathbb{K}$, i.e. $f = c(x-a_1) \cdots (x-a_n)$ for some $c, a_1, \ldots, a_n \in \mathbb{K}$.

The Fundamental Theorem of Algebra states that $\mathbb{C}$ is algebraically closed. This theorem is a kind of a misnomer as $\mathbb{C}$ is a topological construction and its properties depend heavily in particular on the fact that $\mathbb{R}$ is a complete topological space. One can’t thus prove the Fundamental Theorem of Algebra using only algebraic methods. What we will do is that we will prove a related result that is more general and is purely algebraic in nature with an algebraic proof. We will call this the General Fundamental Theorem of Algebra. We will then see that we can deduce the algebraic closure of $\mathbb{C}$ from this result using only a basic result from Analysis (the Intermediate Value Theorem). The following lemma gives us an equivalent description of algebraic closure that we will be using.

Lemma 5.1 A field $\mathbb{K}$ is algebraically closed if and only if there is no proper finite extension $\mathbb{K} \subset \mathbb{F}$.

Proof ($\Rightarrow$). We work with the contrapositive. Suppose there is a finite proper extension $\mathbb{K} \subset \mathbb{F}$. Let $a \in \mathbb{F} \setminus \mathbb{K}$ with minimal polynomial $f$. Then $f$ is irreducible of degree $[\mathbb{K}(a) : \mathbb{K}] \geq 2$ (as $a \notin \mathbb{K}$). In particular $f$ has no root in $\mathbb{K}$. Hence $\mathbb{K}$ is not algebraically closed.

($\Leftarrow$). Again we look at the contrapositive. Suppose that $\mathbb{K}$ is not algebraically closed and let $f$ be a polynomial of degree at least 2 in $\mathbb{K}[x]$ with no root in $\mathbb{K}$. Then we can find a root $a$ in a larger field $\mathbb{F}$. Thus $\mathbb{K} \subset \mathbb{K}(a)$ is a finite proper extension (as $a \notin \mathbb{K}$).

Proposition 5.2 Let $\mathbb{K}$ be a field where $\mathbb{K}^2 = \mathbb{K}$ and where every polynomial of odd degree has a root in $\mathbb{K}$. Then $\mathbb{K}$ is algebraically closed.

Proof Suppose $\mathbb{K} \subseteq \mathbb{F}$ is a finite extension. We want to show that $\mathbb{F} = \mathbb{K}$. By Theorem 3.6 we know that there exists $\theta \in \mathbb{F}$ such that $\mathbb{F} = \mathbb{K}(\theta)$ (notice that $\mathbb{K} \subseteq \mathbb{F}$ is separable as
char $K = 0$). Let $f$ be the minimal polynomial of $\theta$ over $K$. By replacing $F$ by a splitting field of $f$ over $K$ we can assume that $K \subseteq F$ is a Galois extension (note that $f$ is separable as char $K = 0$). Now suppose $[F : K] = 2^rm$ where $m$ is odd. We show that $[F : K] = 1$ in two steps both which involve the Fundamental Theorem of Galois Theory and a group theory result we proved in MA30237: Group Theory.

Step 1. We show that $m = 1$.

Let $G$ be the Galois group of $K \subseteq F$. By the Fundamental Theorem of Galois Theory we have that $|G| = [F : K] = 2^rm$. Let $P$ be a Sylow $2$-subgroup of $G$ and let $M$ be the corresponding subfield of $F$ under the Galois correspondence

$\begin{align*}
F & \quad \{\text{id}\} \\
M & \quad P \\
K & \quad G
\end{align*}$

By the Fundamental Theorem of Galois Theory we have $[M : K] = |G|/|P| = 2^m/2^r = m$. Now let $a \in M$ and let $f_a$ be the minimal polynomial of $a$ over $K$. Then

$$m = [M : K] = [M : K(a)] \cdot [K(a) : K]$$

and thus deg $f_a = [K(a) : K]$ divides $m$. Thus $f_a$ is of odd degree and thus has a root $b \in K$ by our assumptions. As $f_a$ is irreducible (and has $a$ as a root) it follows that $f_a = x - b = x - a$ and $a \in K$. This shows that $M = K$ and thus $m = 1$ and $[F : K] = 2^r$.

Step 2. We show that $r = 0$ and thus $[F : K] = 1$.

We argue by contradiction and suppose that $r \geq 1$. We now have $|G| = [F : K] = 2^r$. By Group Theory there exists an ascending chain of normal subgroups of $G$

$$\{1\} = H_0 < H_1 \ldots < H_r = G$$

where $|H_j| = p^j$. Let $M$ be the subfield of $F$ that corresponds to $H_{r-1}$.

$\begin{align*}
F & \quad \{\text{id}\} \\
M & \quad H_{r-1} \\
K & \quad G = H_r
\end{align*}$

By the Fundamental Theorem of Galois Theory we have that $[M : K] = |G|/|H_{r-1}| = 2^r/2^{r-1} = 2$. Let $a \in M \setminus K$. Then $M = K(a)$. Let $f = x^2 + ax + \beta \in K[x]$ be the minimal polynomial of $a$ over $K$. Then

$$f = (x + \alpha/2)^2 - (\alpha^2/4 - \beta).$$

By our assumptions there is $\gamma \in K$ such that $\gamma^2 = \alpha^2/4 - \beta$. Then

$$f = (x + \alpha/2)^2 - \gamma^2 = (x + \alpha/2 - \gamma)(x + \alpha + \gamma)$$
that is a factorization in \( \mathbb{K}[x] \). This is absurd as \( f \) is irreducible over \( \mathbb{K} \). By this contradiction we know thus that \( r = 0 \) and that \( [F : \mathbb{K}] = 1 \). Hence there is no proper finite extension \( \mathbb{K} \subset F \) and \( \mathbb{K} \) is algebraically closed. \( \square \).

**Remark.** Essentially the Proposition tells us that for a field (of characteristic zero) to be algebraically closed, it suffices that every polynomial in \( \mathbb{K}[x] \) of odd degree has a root in \( \mathbb{K} \) and that every element in \( \mathbb{K} \) has a square root in \( \mathbb{K} \). It will then follow that all polynomials of even degree in \( \mathbb{K}[x] \) have a root as well in \( \mathbb{K} \).

**Theorem 5.3 (The general Fundamental Theorem of Algebra).** Let \( \mathbb{K} \) be a field (of characteristic zero) where \( [\mathbb{K}^* : (\mathbb{K}^*)^2] = 2 \) and

(a) \( \mathbb{K}^* = (\mathbb{K}^*)^2 \cup (-1)(\mathbb{K}^*)^2 \)

(b) \( \mathbb{K}^2 + \mathbb{K}^2 = \mathbb{K}^2 \)

(c) Every polynomial in \( \mathbb{K}[x] \) of odd degree has a root in \( \mathbb{K} \).

Then \( F = \mathbb{K}[x]/\mathbb{K}[x](x^2 + 1) = \mathbb{K}[t] \) (where \( t^2 + 1 = 0 \)) is algebraically closed.

**Proof** Let \( F \subseteq L \) be a finite extension. We want to show that \( L = F \). Much of the proof will go through as it did in the proof of the last proposition. Suppose \( [L : F] = 2^r m \) where \( m \) is odd. Then

\[
[L : \mathbb{K}] = [L : F] \cdot [F : \mathbb{K}] = 2^r m \cdot 2 = 2^{r+1} m.
\]

As in the proof of last proposition we can assume without loss of generality that the extension \( \mathbb{K} \subseteq L \) is a Galois extension. The same argument as was used in Step 1 of that proposition shows that the fact, that all polynomials in \( \mathbb{K}[x] \) of odd degree have a root in \( \mathbb{K} \), implies that \( m = 1 \). We thus have that \( [L : F] = 2^r \). Now the same argument, as was used in Step 2 to deduce that \( r = 0 \) will work here provided that \( F^2 = F \). It thus only remains to see that any \( u = a + tb \) in \( F \) has a square root in \( F \). As (using (a))

\[
\mathbb{K} = (\mathbb{K}^*)^2 \cup (-1)(\mathbb{K}^*)^2 \cup \{0\} = (\mathbb{K}^*)^2 \cup t^2(\mathbb{K}^*)^2 \cup \{0\},
\]

we know that all the elements in \( \mathbb{K} \) have a square root in \( F \). We can thus assume that \( b \neq 0 \).

For any \( v = c + td \) in \( F \) we let \( \bar{v} = c - td \). Notice then that \( v \cdot \bar{v} = c^2 + d^2 \in \mathbb{K}^2 \) by (b), say \( v \cdot \bar{v} = a^2 \) for \( a \in \mathbb{K} \). We will use this fact in the proof.

In particular there is \( c \in \mathbb{K} \) such that \( c^2 = a^2 + b^2 = u \bar{u} \). Notice that as \( b \neq 0 \) we have \( u, \bar{u} \neq 0 \) and thus their product is non-zero giving \( c \neq 0 \). Now \( c \) is in \( \mathbb{K} \) and thus \( c = d^2 \) for some \( d \in F \) and then

\[
u = c(a/c + t(b/c)) = d^2(a/c + t(b/c)).
\]

It thus remains to see that \( a/c + t(b/c) \) has a square root in \( F \). Notice that \( (a/c)^2 + (b/c)^2 = (a^2 + b^2)/c^2 = c^2/c^2 = 1 \). We can thus assume without loss of generality that \( u \cdot \bar{u} = 1 \). Now pick \( \gamma \in \mathbb{K} \) such that \( \gamma^2 = (1 + u)/(1 + \bar{u}) = (1 + a)^2 + b^2 \). Notice that this is non-zero again as \( 1 + u, 1 + \bar{u} \) are nonzero. Then

\[
\frac{(1 + u)}{\gamma} = \frac{(1 + u)(1 + u)}{(1 + u)(1 + \bar{u})} = \frac{(1 + u)u}{(1 + \bar{u})u} = \frac{(1 + u)u}{(u + 1)} = u.
\]

This finishes the proof. \( \square \)
Theorem 5.4  (*The Fundamental Theorem of Algebra*). $\mathbb{C}$ is algebraically closed.

**Proof**  It suffices to show that $\mathbb{K} = \mathbb{R}$ satisfies (a),(b),(c) in Theorem 5.3.

(a) Let $a > 0$ and consider the polynomial $f = x^2 - a \in \mathbb{R}[x]$. Now $f(0) = -a < 0$ and $f(1 + a/2) = 1 + (a/2)^2 > 0$ and thus we know from the Intermediate Value Theorem from Analysis that $f$ has a root $t$. Then $c = t^2$. This shows that $\mathbb{R}^* = \mathbb{R}^+ \cup \mathbb{R}^- = (\mathbb{R}^*)^2 \cup (-1)(\mathbb{R}^*)^2$.

(b) This follows from $\mathbb{R}_0^+ + \mathbb{R}_0^+ = \mathbb{R}_0^+$. Notice that $\supseteq$ follows from $a = a/2 + a/2$.

(c) Consider any monic polynomial $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ of odd degree $n$. If $z \in \mathbb{R}$, then

$$f(z) = z^n(1 + \frac{a_{n-1}}{z} + \cdots + \frac{a_0}{z^n}).$$

We have that $f(z)$ tends to $+\infty$ as $z$ tends to $+\infty$ and (as $n$ is odd) $f(z)$ tends to $-\infty$ as $z$ tends to $-\infty$. Again it follows from the IVT of Analysis that $f$ has a root. $\Box$.

**Definition.** Let $\mathbb{K}$ be a field. A field $\mathbb{F}$ is called an *algebraic closure* of $\mathbb{K}$ if $\mathbb{K} \subseteq \mathbb{F}$ is algebraic and the field $\mathbb{F}$ is algebraically closed.

**Example.** $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$.

**Remark.** We explore algebraic closures a bit further on Problem Sheet 9.
6 Galois’ Theorem

All fields in this chapter are subfields of $\mathbb{C}$.

**Definition.** (a) We say that an extension $K \subseteq F$ is *radical* if there is an ascending chain of fields

$$K \subseteq K(a_1) \subseteq K(a_1, a_2) \subseteq \ldots \subseteq K(a_1, \ldots, a_n) = F$$

such that for each $1 \leq i \leq n$, there exists a prime $p_i$ such that $a_i^{p_i} \in K(a_1, \ldots, a_{i-1})$.

(b) We say that a polynomial $f \in K[X]$ is *solvable by radicals over $K$* if for a splitting field $L$ of $f$ over $K$, there is a radical extension $K \subseteq F$ such that $K \subseteq L \subseteq F$.

**Definition.** We say that a group $G$ is solvable if it has an ascending chain of subgroups

$$\{id\} = H_0 \leq H_1 \leq \ldots \leq H_n = G$$

for which $H_i$ is normal in $H_{i+1}$ for all $i = 0, \ldots, n-1$ and all the factors $H_{i+1}/H_i$ have prime orders.

In this chapter we prove Galois’ Theorem on solvability by radicals. There will be a couple of hurdles that need to be overcome in order to apply the Fundamental Theorem of Galois Theory. One that will involve the roots of unity.

**Theorem 6.1** *(MA30237: Group Theory).* A finite group $G$ is solvable if and only if it has a an ascending chain of subgroups

$$\{id\} = H_0 \leq H_1 \leq \ldots \leq H_n = G$$

for which $H_i$ is normal in $H_{i+1}$ for all $i = 0, \ldots, n-1$ and all the factors $H_{i+1}/H_i$ have prime orders.

In this chapter we prove Galois’ Theorem on solvability by radicals. There will be a couple of hurdles that need to be overcome in order to apply the Fundamental Theorem of Galois Theory. One that will involve the roots of unity.

**Theorem 6.2** Let $F \subseteq \mathbb{C}$ be the splitting field of $x^n - 1$ over $\mathbb{Q}$. Then the Galois group of $\mathbb{Q} \subseteq F$ is isomorphic to $\mathbb{Z}_n^*$.

**Proof** Let $w$ be a root of $\Phi_n$ in $F$. Then the roots of $\Phi_n$ are the elements $w^k$ where $1 \leq k \leq n$ and $(k, n) = 1$. In particular $F = \mathbb{Q}(w)$ and $[F: \mathbb{Q}] = \deg \Phi_n = \phi(n) = |\mathbb{Z}_n^*|$. Now any element in the Galois group must map $w$ to some other root $w^k$, $1 \leq k \leq n$ with $(n, k) = 1$. Thus it is clear that the Galois group $G$ consists of $\sigma_k : F \to F$ where $\sigma_k(w) = w^k$ and $\sigma_k$ fixes $\mathbb{Q}$ pointwise. Finally notice that

$$\Pi : (\mathbb{Z}_n)^* \to G, \ k \mapsto \sigma_k$$

is an isomorphism of groups as $\sigma_k \sigma_r(w) = (w^r)^k = w^{rk} = \sigma_{kr}(w)$. $\square$. 

41
Proposition 6.3 Let $p$ be a prime and $K$ be a field containing $\theta = e^{i2\pi/p}$. Suppose $a \in K \backslash K^p$. If $K \subseteq F$ is normal and $[F : K] = p$, then there exists $t \in F$ such that $F = K(t)$ and $t^p \in K$.

Proof Let $G$ be the Galois group of the extension. By the Fundamental Theorem of Galois Theory we know that $|G| = [F : K] = p$. Thus $G$ is cyclic say $G = \langle \sigma \rangle$ for some $\sigma \in G$. Now $id, \sigma, \ldots, \sigma^{p-1}$ are linearly independent in the vector space of all functions $F \rightarrow F$ (see sheet 10). In particular $id + \theta \sigma + \cdots + \theta^{p-1} \sigma^{p-1} \neq 0$ and thus there exists $z \in F$ such that

$$t = \sum_{k=0}^{p-1} \theta^k \sigma^k(z)$$

is non-zero. Then

$$\sigma(t) = \sum_{k=0}^{p-1} \theta^k \sigma^{k+1}(z)$$

$$= \frac{1}{\theta} \sum_{k=0}^{p-1} \theta^{k+1} \sigma^{k+1}(z)$$

$$= \frac{1}{\theta} \cdot t.$$

As $t$ is not fixed by $\sigma$ we have that $t \in F \backslash K$ and $F = K(t)$. Also $\sigma(t^p) = (\sigma(t))^p = (t/\theta)^p = t^p$ and $t^p \in \text{Fix}(G) = K$ where the last equality holds by the Fundamental Theorem of Galois Theory. □

Proposition 6.4 Let $G$ be a solvable group.

(a) If $H \leq G$, then $H$ is solvable.
(b) If $N \trianglelefteq G$, then $G/N$ is solvable.

Proof See sheet 10.

Definition. Let $F$ be the splitting field of $f \in K[x]$ over $K$. We often call the Galois group of $K \subseteq F$ the Galois group of $f$ over $K$.

Theorem 6.5 (Galois’ Theorem). The polynomial $f \in K[x]$ is solvable by radicals over $K$ if and only if the Galois group of $f$ over $K$ is solvable.

Proof of ($\Leftarrow$). Let $F$ be the splitting field of $f$ over $K$. The aim is to show that we can find a radical extension $K \subseteq L$ such that $K \subseteq F \subseteq L$.

Suppose $[F : K] = n$. By the Fundamental Theorem of Galois Theory we know that $|\text{Aut}_K F| = [F : K] = n$. Let $w = e^{i2\pi/n}$. Then $F(w)$ is the splitting field of $f \cdot (x^n - 1)$ over $K$.

As $K \subseteq F$ is normal, we have (see the proof of the FTGT (4)) that $\sigma(F) = F$ for all $\sigma \in \text{Aut}_K F$. In particular we get a well defined group homomorphism

$$G = \text{Aut}_{K(w)} F(w) \rightarrow \text{Aut}_K F, \sigma \mapsto \sigma|_{F}.$$
This homomorphism is injective as any $\sigma \in G$ that fixes the elements in $\mathbb{F}(w)$ (as it already fixes $w$). Hence $G$ is isomorphic to a subgroup of $\text{Aut}_K\mathbb{F}$ and thus $G$ is solvable by Proposition 6.4. Notice also that Lagrange’s Theorem tells us that $|G|$ divides $n$.

As $G$ is solvable we can apply Theorem 6.1 (from MA30237) that tells us that we have an ascending chain of subgroups

$$\{\text{id}\} = H_0 < H_1 < \cdots < H_m = G$$

where $H_{i-1} \leq H_i$ and $|H_i| / |H_{i-1}| = p_i$ for some primes $p_1, \ldots, p_m$. Let $\mathbb{F}(w) = \mathbb{F}_0, \ldots, \mathbb{F}_m = \mathbb{K}(w)$ be the corresponding subfields of $\mathbb{F}(w)$ under the Galois Correspondence.

$$\begin{align*}
F_0 &= \mathbb{F}(w) & H_0 &= \{\text{id}\} \\
& \vdots & & \vdots \\
F_{i-1} & \leftarrow \Psi & H_{i-1} & \\
& \vdots & & \vdots \\
F_i & & H_i & \\
& \vdots & & \vdots \\
F_m &= \mathbb{K}(w) & G &
\end{align*}$$

By Exercise 1 on Sheet 7 we know that $\mathbb{F}_i \subseteq \mathbb{F}_{i-1}$ is normal as $H_{i-1} \leq H_i$. We also know from the Galois Correspondence that $[\mathbb{F}_{i-1} : \mathbb{F}_i] = |H_i| / |H_{i-1}| = p_i$. As $p_i$ divides $|G|$ (that we have seen previously that divides $n$) we have that $\mathbb{K}(w)$ (and thus $\mathbb{F}_i$) contains $e^{i \cdot \frac{2\pi}{p_i}} = w^{n/p_i}$. We can thus deduce from Proposition 6.3 that $\mathbb{F}_{i-1} = \mathbb{F}_i(t_i)$ for some $t_i \in \mathbb{F}_{i-1}$ where $t_i^{p_i} \in \mathbb{F}_i$. We have thus established that we get a radical chain

$$\mathbb{K}(w) = \mathbb{F}_m \subseteq \cdots \subseteq \mathbb{F}_i \subseteq \mathbb{F}_{i-1} \subseteq \cdots \subseteq \mathbb{F}_0 = \mathbb{F}(w).$$

Now suppose that $n = q_1 \cdots q_s$. Then we get another radical chain

$$\mathbb{K} \subseteq \mathbb{K}(w^{n/q_1}) \subseteq \mathbb{K}(w^{n/q_1q_2}) \subseteq \cdots \subseteq \mathbb{K}(w^{n/q_1 \cdots q_s}) = \mathbb{K}(w).$$

Merging this with the radical chain for $\mathbb{K}(w) \subseteq \mathbb{F}(w)$ we see that $\mathbb{K} \subseteq \mathbb{F}(w)$ is radical and then for the splitting field $\mathbb{F}$ of $f$ we have $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{F}(w)$. $\square$

**Remark.** The proof turned out to be quite fiddly as we needed $\mathbb{K}$ to contain all the $p_i$th roots of unity to be able to use Proposition 6.3. This is a technical hurdle but the core idea of the proof otherwise is the part of the proof that shows that shows that $\mathbb{K}(w) \subseteq \mathbb{F}(w)$ is radical knowing that $\mathbb{K}(w)$ contains all the necessary roots of unity.

**Lemma 6.6** Let $p$ be a prime and let $\mathbb{K}$ be a field that contains $\theta = e^{i \cdot \frac{2\pi}{p}}$. Let $a \in \mathbb{K}$ such that $a$ is not a $p$th power of and element in $\mathbb{K}$ and let $\mathbb{F}$ be a splitting field of

$$f = x^p - a$$

over $\mathbb{K}$. Then the Galois group $G$ of $f$ over $\mathbb{K}$ is cyclic of order $p$. 

43
Proof. Let $b$ be a root of $x^p - a$ in $L$. Then the complete list of roots is

$$b, b\theta, b\theta^2, \ldots, b\theta^{p-1}$$

and $F = \mathbb{K}(b)$ (as $\theta \in \mathbb{K}$). By Sheet 6 (question 5), we have that $x^p - a$ is irreducible. Hence, by the Fundamental Theorem of Galois Theory,

$$|G| = [\mathbb{K}(b) : \mathbb{K}] = p.$$ 

Hence $G$ is cyclic of order $p$. □

Remark. We now want to prove the ($\Rightarrow$) part of Galois’ Theorem. We start thus with a splitting field $F$ of some polynomial over a field $\mathbb{K}$. As the polynomial is solvable by radicals, there is a radical extension $\mathbb{K} \subseteq L$ such that $\mathbb{K} \subseteq F \subseteq L$. Where $F$ lies exactly depends on the given polynomial, but there will be cases where $F = L$. It is thus natural to work with $\mathbb{K} \subseteq L$ instead. The extension $\mathbb{K} \subseteq F$ is a normal extension and thus the Galois group $G$ will be a quotient of $\text{Aut}_{\mathbb{K}L}$ and thus (by Proposition 6.4) $G$ is solvable provided $\text{Aut}_{\mathbb{K}L}$ is solvable.

There is however a problem with this. In order to apply the Fundamental Theorem of Galois Theory we need the radical extension $\mathbb{K} \subseteq L$ to be normal. However this is not true in general. For example the radical extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ is not normal. This problem can though be sorted without much difficulty.

Proposition 6.7 Let $\mathbb{K} \subseteq L$ be a radical extension. Then there exists a field $\mathbb{N}$ such that $L \subseteq \mathbb{N}$ and $\mathbb{K} \subseteq \mathbb{N}$ is a radical extension that is normal.


Proof of Galois’ Theorem ($\Rightarrow$). Let $f \in \mathbb{K}[x]$ that is solvable by radicals. Let $F$ be the splitting field of $f$ over $\mathbb{K}$. Then there is a radical extension $\mathbb{K} \subseteq L$ such that $\mathbb{K} \subseteq F \subseteq L$. By Proposition 6.7 we can assume that $\mathbb{K} \subseteq L$ is normal (and thus a Galois extension). By the remark before Proposition 6.7, it suffices to show that $\text{Aut}_{\mathbb{K}L}$ is solvable. We can thus assume without loss of generality that $\mathbb{K} \subseteq F$ is a radical extension. We thus have a radical chain

$$\mathbb{K} \subseteq \mathbb{K}(t_1) \subseteq \cdots \subseteq \mathbb{K}(t_1, \ldots, t_m) = F$$

where $t_i^{p_i} = a_i \in \mathbb{K}(t_1, \ldots, t_{i-1})$ for some primes $p_1, \ldots, p_m$. We now have similar technical difficulty as in the proof of the ($\Leftarrow$) part. Namely in order to use Lemma 6.6 we need $\mathbb{K}$ to contain all the $p_j$th roots of unity. We overcome this hurdle in a similar way as before. Let $n = p_1 \cdots p_m$ and let $w = e^{2\pi i/n}$. Then $F(w)$ is the splitting field of $f(x^n - 1)$ over $\mathbb{K}$ (and thus also $\mathbb{K}(w)$). Consider now the radical chain

$$\mathbb{K}(w) \subseteq \mathbb{K}(w, t_1) \subseteq \cdots \subseteq \mathbb{K}(w, t_1, \ldots, t_m) = F(w).$$

We can assume here that $t_j \not\in \mathbb{K}(w, t_1, \ldots, t_{j-1})$ (as otherwise the term $\mathbb{K}(w, t_1, \ldots, t_j)$ is redundant and can be omitted). Now let $F_j = \mathbb{K}(w, t_1, \ldots, t_j)$ and let $H_0, H_1, \ldots, H_m$ be the subgroups of $H = \text{Aut}_{\mathbb{K}(w)}F(w)$ that correspond to $F_0, \ldots, F_m$ under the Galois
correspondence.

\[
\begin{array}{c|c}
\mathbb{F}_m = \mathbb{F}(w) & H_m = \{\text{id}\} \\
\vdots & \vdots \\
\mathbb{F}_i & \Phi \\
\mathbb{F}_{i-1} & H_{i-1} \\
\vdots & \vdots \\
\mathbb{F}_0 = \mathbb{K}(w) & H_0 = H
\end{array}
\]

As \( \mathbb{F}_{i-1} \) contains \( \theta = e^{i2\pi/p_i} \) we know that \( \mathbb{F}_i = \mathbb{F}_{i-1}(t_i) \) is the splitting field of \( x^{p_i} - a_i \) over \( \mathbb{F}_{i-1} \) and thus \( \mathbb{F}_{i-1} \subseteq \mathbb{F}_i \) is a normal extension. By Exercise 1 on Sheet 7 we then know that \( H_i \subseteq H_{i-1} \) is normal. By Lemma 6.6 we know also that \( H_{i-1}/H_{i1} \), the Galois group of \( \mathbb{F}_{i-1} \subseteq \mathbb{F}_i \), is cyclic of order \( p_i \). Consider now the larger lattice for \( \mathbb{K} \subseteq \mathbb{F}(w) \).

\[
\begin{array}{c|c}
\mathbb{F}_m = \mathbb{F}(w) & H_m = \{\text{id}\} \\
\vdots & \vdots \\
\mathbb{F}_i & \Phi \\
\mathbb{F}_{i-1} & H_{i-1} \\
\vdots & \vdots \\
\mathbb{F}_0 = \mathbb{K}(w) & H_0 = H
\end{array}
\]

We have that \( \mathbb{K} \subseteq \mathbb{K}(w) \) is normal as the latter field is the splitting field of \( x^n - 1 \) over \( \mathbb{K} \). Thus by Exercise 1 on Sheet 7, we have that \( H \leq G \). By Theorem 6.2 we know that \( G/H \), the Galois group of \( \mathbb{K} \subseteq \mathbb{K}(w) \), is isomorphic to \( \mathbb{Z}_n^* \) and thus in particular abelian. We have thus seen that we get an ascending chain of subgroups of \( G \)

\[ \{\text{id}\} = H_m \leq H_{m-1} \leq \cdots \leq H_0 \leq H_{-1} = G. \]

where \( H_j \leq H_{j-1} \) for \( j = m, \ldots, 0 \) and where \( H_{j-1}/H_j \) is abelian. Thus \( G \) is solvable.

Finally \( \text{Aut}_\mathbb{K}\mathbb{F} \) is isomorphic to a quotient of \( G \) (by the Fundamental Theorem of Galois Theory) as \( \mathbb{K} \subseteq \mathbb{F} \) is normal. Hence the Galois group of \( \mathbb{K} \subseteq \mathbb{F} \) is solvable. \( \Box \)

Galois Theory originated from the failed attempt to solve the quintic by radicals and it is thus appropriate to end by giving an example of an unsolvable quintic over \( \mathbb{Q} \).

**An unsolvable quintic over \( \mathbb{Q} \).**

Recall from Group Theory that the group \( S_n \) is solvable if and only if \( n \leq 4 \). We have seen earlier (Proposition 2.18) that if \( f \in \mathbb{K}[x] \) has \( n \) distinct roots (that happens
for example if \( f \) is irreducible), then the Galois group is isomorphic to a subgroup of \( S_n \). Hence all polynomials of degree less than or equal to 4 are solvable by radicals.

We now want to find an example of a polynomial \( f \in \mathbb{Q}[x] \) of degree 5, whose Galois group is \( S_5 \) and thus \( f \) not solvable by radicals.

**Lemma 6.8** Let \( p \) be a prime and suppose that \( H \) is a subgroup of \( S_p \) that contains a 2-cycle and such that \( |H| \) is divisible by \( p \). Then \( H = S_p \).

**Proof** (See Problem Sheet 10)

**Proposition 6.9** Let \( p \) be a prime and let \( f \) be an irreducible polynomial of degree \( p \) over \( \mathbb{Q} \) that has precisely two non-real roots in \( \mathbb{C} \). Then the Galois group \( G \) of \( f \) over \( \mathbb{Q} \) is isomorphic to \( S_p \).

**Proof** Let \( F \) be the splitting field of \( f \) over \( \mathbb{Q} \) and let \( \tau : \mathbb{C} \to \mathbb{C}, z \mapsto \bar{z} \) be the complex conjugation. Then the restriction \( \tau|_F \in G \) fixes all the real roots and swaps the two non-real roots. It follows that \( G \) (thought of as a permutation of the roots) contains a 2-cycle. Let \( a \) be any root of \( f \) in \( F \). Then \( [\mathbb{Q}(a) : \mathbb{Q}] = p \) as \( f \) is irreducible. Consider the chain \( \mathbb{Q} \subseteq \mathbb{Q}(a) \subseteq F \).

The tower law gives that \( p \) divides \([F : \mathbb{Q}]\). But by the Fundamental Theorem of Galois Theory we have that the latter is equal to \( |G| \). Thus \( G \) is a subgroup of \( S_p \), that contains a 2-cycle and whose order is divisible by \( p \). By Lemma 6.8 it follows that \( G = S_p \).

It is now easy to find an explicit example of quintic over \( \mathbb{Q} \) that is not solvable by radicals.

**Example.** The polynomial \( f = x^5 - 6x + 3 \) is not solvable by radicals. (See Problem Sheet 10)