The University of Birmingham
School of Mathematics

Galois Theory

These are the lecture notes for the Galois Theory course taught in the Spring of 2006 by Sergey Shpectorov. They are based on the notes written by David Craven of the course taught in the Spring of 2003 by Prof. John Wilson and in 2004 by Dr Gerhard Röhrle.

Contents

Chapter 1

Field extensions

1.1 Fields, subfields, extensions

Definition 1.1.1 *A* field *is a commutative ring L such that every $a \in L^* = L \setminus \{0\}$ is a unit, that is, it has a multiplicative inverse a^{-1}.*

We will also write $\frac{1}{a}$ for a^{-1}.

Example 1.1.2

1. $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{C}$ are fields with respect to the operations of addition and multiplication.

2. $\mathbb{Z}$ is not a field, as the only nonzero integers that have multiplicative inverse in $\mathbb{Z}$ are ± 1. However, the quotient ring $\mathbb{Z}/p\mathbb{Z}$ is a field, where p is a prime. It is often denoted by $\mathrm{GF}(p)$ or, in this course, by $\mathbb{F}_p$. $\mathbb{F}_p$ is a *finite field*, as it has a finite number of elements, p.

3. Let K be any field, and form the polynomial ring in n indeterminates $K[x_1, x_2, \ldots, x_n]$. Then the field of fractions of this polynomial ring is called the *rational function field* in $x_1, x_2, \ldots, x_n$. Then $K(x_1, x_2, \ldots, x_n) = \{\frac{f}{g} \mid f, g \in K[x_1, x_2, \ldots, x_n],\, g \neq 0\}$.

Definition 1.1.3 *Let L be a field. A* subfield *is a subring K which is a field with respect to the operations inherited from L.*

To see that $K \subseteq L$ is a subfield of L, it suffices to check the following:

1. $0, 1 \in K$;
2. if $k_1, k_2 \in K$ then $k_1 - k_2, k_1k_2 \in K$;
3. if $k \in K \setminus \{0\}$ then $k^{-1} \in K$.

In Galois theory, we are often concerned with constructing fields containing a given field K. It is because of this, that we want an opposite notion to that of a subfield. If K is a subfield of L then we say that L is a *field extension* (or just an *extension*) of K. We may also refer to the pair $K \subseteq L$ as to a field extension. One more notation for such a pair is L/K (pronounced "*L over K*"). This is not to be mixed with the notation for the factor rings.

Example 1.1.4 1. $\mathbb{C}$ is an extension of $\mathbb{R}$ and $\mathbb{Q}$, and $\mathbb{R}$ is an extension of $\mathbb{Q}$. We can express all of these at once by writing down a *tower* of extensions $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

2. Let $M = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$. Then M is a subfield of $\mathbb{R}$ containing $\mathbb{Q}$, hence it is a field extension of $\mathbb{Q}$ (and $\mathbb{R}$ is a field extension of M). Indeed, M clearly contains $\mathbb{Q}$. So we just need to see that M is a subfield. Manifestly, M is closed under subtraction and also it is closed under multiplication (indeed, multiply two arbitrary elements of M and then expand the product using $(\sqrt{2})^2 = 2$; the results will again be of the form $a+b\sqrt{2}$ for suitable $a, b \in \mathbb{Q}$). This means that M is a subring of $\mathbb{R}$. Since $\mathbb{R}$ is commutative, so is M. Finally, if $u = a + b\sqrt{2} \in M$ and $u \neq 0$ then u^{-1} (as defined in $\mathbb{R}$) is equal to $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2} \in M$. (Here we use that $a^2 - 2b^2 \neq 0$, since $\sqrt{2}$ is irrational.) Thus, M is a commutative subring, in which every nonzero element is a unit, that is, M is a field.

3. To see that $L = \{a + b2^{1/3} + c2^{2/3} \mid a, b, c \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$, and an extension of $\mathbb{Q}$, we first show (similarly to the above) that L is a subring of $\mathbb{R}$. For the final statement, that every nonzero element $u \in L$ is a unit, we have to use a more elaborate proof, involving linear algebra. Consider the map $\theta : x \mapsto ux$ from L to L. This map is $\mathbb{Q}$-linear, since for $a, b \in \mathbb{Q}$ and $v, w \in L$ we have

$$\begin{aligned} \theta(av + bw) &= u(av + bw) \\ &= a(uv) + b(uw) \\ &= a\theta(v) + b\theta(w). \end{aligned}$$

The map θ is also injective, since if $\theta(v) = 0$, we have $uv = 0$ with u non-zero, and so $v = 0$, giving a trivial kernel for θ.

The rank–nullity formula says that if $\phi : U \to V$ is linear and $\dim U$ is finite, then the rank of ϕ (dimension of $\operatorname{im} \phi$) plus the nullity of ϕ (dimension of $\ker \theta$) is equal to $\dim U$. In our example, L is finite dimensional, of dimension (at most) three over $\mathbb{Q}$. Also, the nullity of θ is zero, and so $\operatorname{im} \theta$ is a subspace of L of dimension equal to $\dim L$. Thus, $\operatorname{im} \theta = L$, that is, θ is surjective. In particular, there exists an element $v \in L$ such that $\theta(v) = 1$; but then $uv = 1$, and v is the inverse of u.

1.2 Degree of extension, finite extensions

Linear algebra plays an important role in the Galois Theory. Suppose $K \subseteq L$ is a field extension. We can view L as a vector space over K as follows: The addition in the vector space L is the usual addition in L, while the scalar multiplication (scalars are elements of K) is the restriction of the usual multiplication from L to the set of pairs (a, v), where $a \in K$ (a scalar) and $v \in L$ (a vector).

Definition 1.2.1 *Let L be a field extension of K. If $\dim_K L$ is finite we say that L is a* finite extension *of K, or that L over K is a finite extension. Then the* degree *of the extension, written $[L : K]$ is the dimension $\dim_K L$. If L is infinite dimensional over K then we write $[L : K] = \infty$.*

Example 1.2.2

1. For any field K, we have $[K : K] = 1$. Reversely, if $[L : K] = 1$ then $L = K$.
2. $[\mathbb{C} : \mathbb{R}] = 2$; a basis for this vector space is $\{1, i\}$.
3. Let M be as in Example 1.1.4(2). Then $[M : \mathbb{Q}] = 2$, and as a basis for M over $\mathbb{Q}$, one may choose $\{1, \sqrt{2}\}$.
4. Let L be as in Example 1.1.4(3). Then $[L : \mathbb{Q}] = 3$; a basis for this vector space is $\{1, 2^{1/3}, 2^{2/3}\}$.
5. We know that π is transcendental, that is, it is not a root of any nonzero polynomial from $\mathbb{Q}[x]$. This implies that all powers of π, $\{1, \pi, \pi^2, \pi^3, \dots\}$, are linearly independent over $\mathbb{Q}$. Thus, $[\mathbb{R} : \mathbb{Q}] = \infty$ (and also $[\mathbb{C} : \mathbb{Q}] = \infty$).

The degree of the field extension provides a measure of how "big" the extension is. Suppose we are given a tower of finite extensions. The following important result tells us how the degrees combine.

Theorem 1.2.3 [Tower Law for Finite Field Extensions] *Let L be a finite extension of K, and M be a finite extension of L. Then*

$$[M : K] = [M : L][L : K].$$

In particular, M is a finite extension of K.

Proof: Let $\{e_1, e_2, \dots, e_n\}$ be a basis of M over L and $\{f_1, f_2, \dots, f_m\}$ be a basis of L over K. Since $[M : L] = n$ and $[L : K] = m$, in order to show that $[M : K] = [M : L][L : K] = mn$, it suffices to establish that

$$T = \{e_i f_j \mid 1 \le i \le n, 1 \le j \le m\}$$

is a basis for M over K. Let u be an element of M. Write $u = \sum_{i=1}^{n} a_i e_i$, with $a_i \in L$. Then each a_i can be expressed in the form

$$a_i = \sum_{j=1}^{m} b_{ij} f_j,$$

with $b_{ij} \in K$. We can substitute this expression for a_i into our expression for u to get

$$u = \sum_{i=1}^{n} \sum_{j=1}^{m} b_{ij} f_j e_i = \sum_{i,j} b_{ij} e_i f_j.$$

Thus, T spans M as a vector space over K.

Now we prove that the set T is linearly independent over K. Suppose that

$$\sum_{i,j} c_{ij} e_i f_j = 0,$$

with each $c_{ij} \in K$. For each i, write

$$w_i = \sum_{j=1}^{m} c_{ij} f_j,$$

and notice that each $w_i \in L$. Then

$$\sum_{i=1}^{n} w_i e_i = \sum_{i,j} c_{ij} e_i f_j = 0,$$

and so $\sum_{i=1}^{n} w_i e_i = 0$. Since $\{e_1, e_2, \ldots, e_n\}$ is a basis for M over L, $w_i = 0$ for all i, yielding $\sum_{j=1}^{m} c_{ij} f_j = 0$ for all i. So, since $\{f_1, f_2, \ldots, f_m\}$ is a basis for L over K, we conclude that each $c_{ij} = 0$, as required. □

1.3 Adding elements to a field

Suppose $K \subseteq L$ is a field extension and suppose A be a subset of L. In this section we construct an intermediate field $M = K(A)$ ("intermediate" means that $K \subseteq M \subseteq L$), obtained by "adding" the elements of A to K.

Lemma 1.3.1 *Let L be a field and $\{F_\lambda\}_{\lambda \in \Lambda}$ be a family of subfields. Then $\bigcap_\lambda F_\lambda$ is also a subfield.*

Proof: Let $F = \bigcap_\lambda F_\lambda$. We have that $0,\, 1 \in F_\lambda$ for all λ, and so $0,\, 1 \in F$. Let $k_1,\, k_2 \in F$ with $k_2 \neq 0$. Then k_1 and k_2 are in each F_λ and so $k_1 - k_2 \in F_\lambda$ and $k_1 k_2^{-1} \in F_\lambda$ for each λ, and so they are both elements of F. Hence F is a subfield. □

Theorem 1.3.2 *Let L be an extension of K, and $A \subseteq L$ be a subset. Among all subfields of L containing K and A, there is a unique minimal one, denoted $K(A)$. The minimality of $K(A)$ means that if $M \subseteq L$ is a subfield containing $K \cup A$ then $K(A) \leq M$.*

Proof: Consider the family $\{F_\lambda\}_{\lambda \in \Lambda}$ of all subfields of L containing $K \cup A$. Since $K \cup A \subseteq L$, we have that L itself is in this family, and so this family is non-empty. Let $F = \bigcap_\lambda F_\lambda$. By Lemma 1.3.1, F is a subfield of L. Since $K \cup A \subseteq F_\lambda$ for all λ, $K \cup A \subseteq F$, that is, F belongs to the family $\{F_\lambda\}$. Finally, suppose $K \cup A \subseteq M$, where M is a subfield of L. Then $M = F_\lambda$ for some λ, and so it contains F. □

Definition 1.3.3 *The subfield $K(A)$ is called the subfield* generated by A over K. *If $A = \{a_1, a_2, \ldots, a_n\}$ then we simply write $K(a_1, a_2, \ldots, a_n)$ in place of $K(\{a_1, a_2, \ldots, a_n\})$.*

Example 1.3.4

1. Since $\mathbb{C}$ is the only subfield of itself containing $\mathbb{R}$ and i, we have by definition that $\mathbb{C} = \mathbb{R}(i)$. To determine $\mathbb{Q}(i)$, observe that every subfield containing $\mathbb{Q}$ and i also contains all elements of $M = \{a + bi \,|\, a, b \in \mathbb{Q}\}$. So it suffices to see that this subset, M, is in fact a subfield. First of all, M is a subring, since it is closed with respect to subtraction and multiplication. Thus, we just need to see that for every $u \in M$, the inverse u^{-1} (as found in $\mathbb{C}$) is also contained in M. Notice that $(a + bi)^{-1} = \frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2} i \in M$. Hence M is a subfield, smallest among the subfields containing $\mathbb{Q}$ and i. Thus, $\mathbb{Q}(i) = M = \{a + bi \,|\, a, b \in \mathbb{Q}\}$. The field $\mathbb{Q}(i)$ has a special name, it is called the field of *Gaussian numbers*.

2. The field $M = \{a + b\sqrt{2}\}$ from Example 1.1.4 (ii) is in fact $\mathbb{Q}(\sqrt{2})$.

3. Similarly, the field $L = \{a + b2^{\frac{1}{3}} + c2^{\frac{2}{3}} \,|\, a, b, c \in \mathbb{Q}\}$ from Example 1.1.4 (iii) is simply $\mathbb{Q}(2^{\frac{1}{3}})$.

4. One can show that $\mathbb{Q}(\sqrt{2}, i) = \{a + b\sqrt{2} + ci + di\sqrt{2} \,|\, a, b, c, d \in \mathbb{Q}\}$.

We will now present a number of simple, but important observations concerning generation of fields.

Proposition 1.3.5 *Suppose L is an extension of K and A and B are two subsets of L. If $B \subseteq K(A)$ then $K(B)$ is a subfield of $K(A)$.*

Proof: Since $K(A)$ contains K and, by condition, contains B, it follows from the definition of $K(B)$ that $K(B) \subseteq K(A)$. □

Corollary 1.3.6 *Suppose L is an extension of K and A and B are two subsets of L. If $B \subseteq K(A)$ and $A \subseteq K(B)$ then $K(A) = K(B)$.* □

This shows that the same extension can be generated by many different sets of elements.

Example 1.3.7 1. Since $\sqrt{2}i$ is contained in $\mathbb{Q}(\sqrt{2}, i)$, we conclude that $\mathbb{Q}(\sqrt{2}i) \subseteq \mathbb{Q}(\sqrt{2}, i)$. It can be shown that neither $\sqrt{2}$, nor i is contained in $\mathbb{Q}(\sqrt{2}i)$, so the inclusion is strict.

2. Clearly, $1 + i \in \mathbb{Q}(i)$, but also $i = (1 + i) - 1 \in \mathbb{Q}(1 + i)$. This means that $\mathbb{Q}(i) = \mathbb{Q}(1 + i)$. In fact, $\mathbb{Q}(i) = \mathbb{Q}(a + bi)$ for all $a, b \in \mathbb{Q}$, with $b \neq 0$.

3. Here is a more complex example: Let $A = \{\pm\sqrt[4]{2}, \pm\sqrt[4]{2}i\}$ be the set consisting of the four complex roots (zeros) of the polynomial $x^4 - 2$. Let $L = \mathbb{Q}(A)$ (as a subfield of $\mathbb{C}$). Let $B = \{\sqrt[4]{2}, \sqrt[4]{2}i\}$. Then B contains only two of the roots, but $L = \mathbb{Q}(A) = \mathbb{Q}(B)$. Indeed, $B \subseteq A$ and so $\mathbb{Q}(B) \subseteq \mathbb{Q}(A)$. On the other hand, $-\sqrt[4]{2} \in \mathbb{Q}(B)$, since $\sqrt[4]{2} \in B$,

and similarly, $-\sqrt[4]{2}i \in \mathbb{Q}(B)$, since $\sqrt[4]{2}i \in B$. Thus, $A \subseteq \mathbb{Q}(B)$, and so $\mathbb{Q}(A) = \mathbb{Q}(B)$ by Corollary 1.3.6. Thus, we only need two of the four roots to generate L.

Furtheremore, let $C = \{\sqrt[4]{2}, i\}$. Clearly, $B \subseteq \mathbb{Q}(C)$, since $\sqrt[4]{2} \in C$, while $\sqrt[4]{2}i$ is the product of $\sqrt[4]{2}$ and i. Reversely, since $\sqrt[4]{2} \in B$ and $i = \frac{\sqrt[4]{2}i}{\sqrt[4]{2}}$, we also have $C \subseteq \mathbb{Q}(B)$. Thus, we can also write $L = \mathbb{Q}(C)$. In particular, L contains $\mathbb{Q}(i)$, the Gaussian numbers.

The final observation demonstrates then one does not need to add all generators at once, but rather can increase the field in steps.

Proposition 1.3.8 *Suppose $L = K(A)$, where $A = A_1 \cup A_2$. Then $M = K(A_1)$ is a subfield of L, and furthermore, $L = M(A_2)$.*

Proof: Since $A_1 \subseteq A$, Proposition 1.3.5 implies that $M \subseteq L$. Since L contains M and A_2, we have $M(A_2) \subseteq L$. On the other hand, $M(A_2)$ contains A_2, and also $M(A_2)$ contains M, which contains K and A_1. Hence, $M(A_2)$ contains K and $A = A_1 \cup A_2$, and hence $M(A_2)$ contains $L = K(A)$. □

Example 1.3.9 The extension $\mathbb{Q}(\sqrt{2}, i)$ of $\mathbb{Q}$ can be viewed as the extension $\mathbb{Q}(i)(\sqrt{2})$, that is, it is generated by $\sqrt{2}$ over the Gaussian numbers. Another way to look at it is that it is generated by i over the (fully real) subfield $\mathbb{Q}(\sqrt{2})$.

Chapter 2

Polynomials, evaluation, minimal polynomial

2.1 Ring of polynomials

Let K be a field. A *polynomial* in the indeterminate x over K of *degree* $n \geq 0$ is a formal expression $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, where all $a_i \in K$, and $a_n \neq 0$. The zero polynomial is $a_0 = 0$, and its degree is defined to be $-\infty$. The degree of a polynomial f is denoted $\deg(f)$. The polynomials of degree zero and the zero polynomial are called the *constant polynomials*. In general, the a_is are called the coefficients of the polynomial and, if the degree n is greater than or equal to zero, then a_n is called the *leading coefficient* and $a_n x^n$ is called the *leading term* of the polynomial. The zero polynomial has no leading coefficient. If the leading coefficient of a polynomial is equal to one (that is, 1_K) then the polynomial is called *monic*.

Polynomials in x form a commutative ring with respect to the usual addition and multiplication. This ring is denoted $K[x]$. We identify every $a \in K$ with the corresponding constant polynomial. Under this identification, K is a subring of $K[x]$. Similarly, for a field extension $K \subseteq L$, we can view $K[x]$ as a subring of $L[x]$. That is, every polynomial over K is at the same time a polynomial over L.

In the remainder of this section we review without proofs some properties of the ring of polynomials $K[x]$.

We first remark that the degree function on polynomials satisfies the following rules:

$$\deg(f+g) \leq \max(\deg(f), \deg(g)),$$
$$\deg(fg) = \deg(f) + \deg(g).$$

The second of these rules implies that $K[x]$ is an *integral domain*, *i.e.*, a commutative ring with one, that has no zero divisors. The latter condition means that if $fg = 0$, for $f, g \in K[x]$, then $f = 0$, or $g = 0$.

We next review the Euclidean Algorithm for polynomials.

Proposition 2.1.1 (Euclidean Algorithm) *If $f, g \in K[X]$ with $g \neq 0$, then there exist unique $q, r \in K[X]$ with $\deg(r) < \deg(g)$, such that $f = qg + r$.* □

Recall that an *ideal* I of a commutative ring R (such as, say, the ring of polynomials, $K[x]$) is an additive subgroup of R, such that for all elements $r \in R$ and $i \in I$ we have that ri is again in I.

An application of the Euclidean Algorithm yields the following important result.

Theorem 2.1.2 *If K is a field then $K[x]$ is a* principal ideal domain*, that is, for every ideal I of $K[x]$ there is a polynomial $p \in K[x]$ such that I is expressible as*

$$I = (p) = pK[x] = \{pf \mid f \in K[x]\}.$$

□

We remark that if $I \neq \{0\}$ then the polynomial p is always a nonzero polynomial of the smallest possible degree in I. All such polynomials in I differ only by a constant factor, and exactly one of them is monic.

If I is an ideal of a (commutative) ring R then the *factor ring* R/I has as elements all *cosets* $a + I = \{a + i \mid i \in I\}$ for $a \in R$. The operations on R/I are defined by: $(a+I)+(b+I) = a+b+I$ and $(a+I)(b+I) = ab+I$.

Recall that an ideal I of R is *maximal* if the only ideal of R properly containing I is R itself.

Proposition 2.1.3 *Suppose R is a commutative ring with one and I is an ideal of R. Then R/I is a field if and only if I is a maximal ideal.* □

Since we are going to apply this theorem with $R = K[x]$, we need to know which ideals of $K[x]$ are maximal. Recall that a nonconstant polynomial $f \in K[x]$ is *irreducible* if, whenever $f = gh$ for $g, h \in K[x]$, we have that g is constant (and hence $\deg(h) = \deg(f)$, or h is constant (and hence $\deg(g) = \deg(f)$).

Proposition 2.1.4 *An ideal (p) of $F[x]$ is maximal if and only if p is an irreducible polynomial.* □

2.2 Roots (zeros) of polynomials

Consider a field extension $K \subseteq L$ and suppose $f = \sum_{i=0}^{n} a_i x^i \in K[x]$. For $u \in L$, we write $f(u)$ for the *value* of the polynomial f at $x = u$, that is, the element of L given by

$$f(u) = \sum_{i=0}^{n} a_i u^i.$$

An element $u \in L$ is a *root* (or a *zero*) of f if and only if $f(u) = 0$.

Proposition 2.2.1 *For a field extension $K \subseteq L$, if $f \in K[x]$ has a root $u \in L$ then $f = (x - u)q$ for a unique $q \in L[x]$. Furthermore, $u \in K$ if and only $q \in K[x]$.*

Proof: By the Euclidean Algorithm, there exist unique $q, r \in L[x]$ such that $\deg(r) < 1 = \deg(x - u)$ and $f = q(x - u) + r$. Since $\deg(r) < 1$, the polynomial r is a constant polynomial. Evaluating both sides at $x = u$ yields

$$0 = f(u) = q(u)(u - u) + r.$$

Hence $r = 0$. If $u \in K$ then the above applies to $L = K$, which means that the unique q (and $r = 0$) are in fact in $K[x]$. Similarly, if $q \in K[x]$ then q' and r', such that $\deg(r') < \deg(q)$ and $f = q'q + r'$, are unique regardless of whether we apply the Euclidean Algorithm to $K[x]$, or to $L[x]$. This means that q' and r' lie, in fact, in $K[x]$. Now, since $f = (x-u)q$, we have that $r' = 0$ and $q' = x - u$. Thus, $x - u \in K[x]$, and hence $u \in K$. □

Polynomials of degree one are called *linear* polynomials, and hence factors $x - u$ in a polynomial f will be called *linear factors* of f. Proposition 2.2.1 tells us that a polynomial $f \in K[x]$ has linear factors in $L[x]$ if and only if f has a root in L.

Corollary 2.2.2 *Suppose $F \subseteq L$ is a field extension, and let $u_1, u_2, \ldots, u_k$ be all roots of $f \in K[x]$ in L. Then*

$$f = (x-u_1)^{s_1} \cdots (x-u_k)^{s_k} g,$$

where all $s_i \geq 1$, $g \in L[x]$ and g has no root in L.

In particular, f has at most $\deg(f)$ *roots in L.*

Proof: Decompose f in $L[x]$ as a product $(x-v_1)^{s_1} \cdots (x-v_m)^{s_m} g$ with as many linear factors as possible (as big $s_1 + \cdots + s_m$ as possible). Here all v_i are distinct and $s_i \geq 1$. Since $s_1 + \cdots + s_m$ is maximal possible, g cannot have a linear factor in $L[x]$, which means, by Proposition 2.2.1, that g has no root in L. Clearly, $v_1, \ldots, v_m$ are roots of f and so every v_i lies in $\{u_1, \ldots, u_k\}$. Assuming that some u_i does not belong to $\{v_1, \ldots, v_m\}$, evaluate f at $x = u_i$. This gives $0 = f(u_i) = (u_i - v_1)^{s_1} \cdot (u_i - v_m)^{s_m} g(u_i)$, yielding $g(u_i) = 0$, since none of the factors $u_i - v_j$ is zero. However, g has no root in L, a contradiction. Thus, $k = m$, and up to reordering, $u_i = v_i$ for all i.

The last claim follows, since $k \leq s_1 + \cdots + s_k \leq \deg(f)$. □

Roots are useful when we need to verify irreducibility of a polynomial of a low degree. The proof of the following result is left to the reader as an exercise.

Proposition 2.2.3 *Suppose $f \in K[x]$ and* $\deg(f) \leq 3$ *then f is irreducible in $K[x]$ if and only if f has no root in K.* □

Example 2.2.4 1. The roots of $f = x^2 + 1$ in $\mathbb{C}$ are $\pm i$. Neither of the two roots is in $\mathbb{Q}$, hence f is irreducible over $\mathbb{Q}$ by Proposition 2.2.3. Similarly, f is irreducible over $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(2^{\frac{1}{3}})$. However, $\mathbb{Q}(i)$

(and an even larger field $\mathbb{Q}(\sqrt{2}, i)$) contains the roots of f and so f is not irreducible over $\mathbb{Q}(i)$ (and $\mathbb{Q}(\sqrt{2}, i)$). In fact, over these fields $f = x^2 + 1 = (x - i)(x + i)$ can be written as a product.

2. The polynomial $g = x^3 - 5x^2 + 2x + 2$ has root 1. Hence it is not irreducible even over $\mathbb{Q}$. Since 1 lies in every field, g is always reducible. In fact, $x^3 - 5x^2 + 2x + 2 = (x - 1)(x^2 - 4x - 2)$.

3. When the degree of the polynomial is greater than three, the conclusion of Proposition 2.2.3 becomes wrong. For example, $x^4 - 4$ has no roots in $\mathbb{Q}$, but it is not irreducible. Indeed, $x^4 - 4 = (x^2 - 2)(x^2 + 2)$.

4. If we interpret $f = x^2 + 1$ as a polynomial over $\mathbb{F}_p$, p a prime, is this polynomial irreducible or not? It depends on p. For example, over $\mathbb{F}_2$ the polynomial f is equal to $(x - 1)^2$ (1 is a double root), while over $\mathbb{F}_3$ f again has no roots, and hence it is again irreducible.

5. Similarly, irreducibility of $f = x^2+x+1$ over $\mathbb{F}_p$ depends on p. However, this time f has no roots in $\mathbb{F}_2$ and hence it is irreducible over this field, while over $\mathbb{F}_3$ it is reducible, since 1 is a root. In fact, $x^2 + x + 1 = x^2 - 2x - 1 = (x - 1)^2$ in $F_3[x]$.

2.3 Evaluation map, minimal polynomial

Definition 2.3.1 *Let again $K \subseteq L$ be a field extension and $u \in L$. The function $\epsilon_u : K[x] \longrightarrow L$ defined by $f \mapsto f(u)$ is called the* evaluation map *at $u \in L$.*

Proposition 2.3.2 *The evaluation mapping ϵ_u is a ring homomorphism.*

Proof: Indeed, $\epsilon_u(f + g) = (f + g)(u) = f(u) + f(u) = \epsilon_u(f) + \epsilon_u(g)$ and similarly for the product. □

Since ϵ_u is a homomorphism, its kernel, $\ker\epsilon_u = \{f \in K[x] \mid \epsilon_u(f) = 0\}$, is an ideal of $K[x]$. Set $I = I_u = \ker\epsilon_u$. Since $\epsilon_u(f) = 0$, the ideal I consists of all polynomials from $f \in K[x]$, such that $f(u) = 0$.

We now recall from Section 2.1 that $K[x]$ is a principal ideal domain (PID). Therefore, I is a principal ideal, namely, either $I = \{0\}$ or $I = (f)$, where $f \in I$ is a nonzero polynomial of the smallest possible degree. Since this f is only defined up to a constant factor, we prefer to make it unique by requiring that f be monic.

This discussion show that there are two completely different possibilities:

Definition 2.3.3 *Either $I_u = \{0\}$, which means that there exists no polynomial in $K[x]$, for which u is a root, or such polynomials exist and so $I_u \neq \{0\}$. In the first case, u is called* transcendental *over K; in the second case u is* algebraic *over K.*

If u is algebraic then there exists a unique monic polynomial $p \in K[x]$ (in fact, $p \in I_u$), such that $I_u = (p)$. This polynomial p is called the minimal polynomial of u over K. Its definition can be restated as follows:

Definition 2.3.4 *The* minimal polynomial *of u over K is the monic polynomial $p \in K[x]$ of the smallest possible degree, such that u is a root of f.*

We will use a special notation for the minimal polynomial, $\min_{u,K}$. In order to work effectively with the minimal polynomial, we need to know its properties.

Proposition 2.3.5 *Suppose $K \subseteq L$ is a field extension and $u \in L$ is algebraic over K. Set $p = \min_{u,K}$.*

1. *If $u \in K$ then $p = x - u$; if $u \notin K$ then $\deg(p) \geq 2$.*

2. *p is irreducible over K.*

3. *If $f \in K[x]$ and $f(u) = 0$ then p divides f.*

Proof: We start with claim 2. Suppose $p = gh$ for some $g, h \in K[x]$. Since $p \neq 0$, both g and h are nonzero. Since $p(u) = 0$, we have $(gh)(u) = g(u)h(u) = 0$ and hence $g(u) = 0$ or $h(u) = 0$. Without loss of generality we may assume that $g(u) = 0$, that is, $g \in I_u$. Since p has the smallest degree among the nonzero polynomials from I_u, we conclude that $\deg(g) \geq \deg(p)$. This means that $\deg(g) = \deg(p)$ and $\deg(h) = 0$, that is, h is a constant polynomial. This proves that p is irreducible.

For claim 3, suppose $g \in K[x]$ and $g(u) = 0$. By the Euclidean Algorithm, there exist $q, r \in K[x]$ with $\deg(r) < \deg(p)$, such that $g = qp + r$. Evaluating at $x = u$ gives $0 = q(u)0 + r(u)$, that is, $r(u) = 0$ and hence $r \in I_u$. Since $\deg(r) < \deg(p)$ and since p has the minimal degree among all nonzero elements of I_u, we conclude that $r = 0$. Thus, $g = qp$, that is, p divides g.

Finally, if $u \in K$ then $x - u \in K[x]$. Clearly, u is a root of $x - u$, hence $x - u \in I_u$. Since no nonzero polynomial in I_u can have degree less than $1 = \deg(x - u)$, we have $p = x - u$. If $u \notin K$, then u cannot be a root of a linear polynomial from $K[x]$. Hence, $\deg(p) \geq 2$. □

Let us now see some examples.

Example 2.3.6

1. First of all, π is transcendental. The powers of π are linearly independent over $\mathbb{Q}$. The minimal polynomial $\min_{\pi,\mathbb{Q}}$ is not defined.

2. Since i is a root of $x^2 + 1$, which is a monic of degree two, we see i is algebraic over $\mathbb{Q}$ and that $\min_{i,\mathbb{Q}} = x^2 + 1$. Indeed, if this polynomial were not the minimal polynomial, then the minimal polynomial would have degree less then two (that is, it would have to have degree one). However, this is only possible if $i \in \mathbb{Q}$, which is not the case. Similarly, $x^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}(\sqrt{2})$, since $i \notin \mathbb{Q}(\sqrt{2})$. This also means that $x^2 + 1$ is irreducible over both $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$. However, $x^2 + 1$ is not irreducible over $\mathbb{Q}(i)$ and indeed the minimal polynomial of i over $\mathbb{Q}(i)$ is $x - i$. Since i is still a root of $x^2 + 1$, we must have that $x - i$ divide $x^2 + 1$, and indeed, $x^2 + 1 = (x - i)(x + i)$.

3. Similarly, $x^2 - 2$ is the minimal polynomial of $u = \sqrt{2}$ over $\mathbb{Q}$, since $u \notin \mathbb{Q}$ and u is a root of $x^2 - 2$. Furthermore, $x^2 - 2$ divides every polynomial from $\mathbb{Q}[x]$, of which u is a root. Also, $x^2 - 2$ is irreducible over $\mathbb{Q}$ and it remains irreducible over $\mathbb{Q}(i)$.

4. Observe that $x^3 + 2x - x - 1$ is irreducible over $\mathbb{Q}$. Let u be one of its roots from $\mathbb{C}$. Although we don't know a nice expression for u itself, but we can claim that $x^3 + 2x^2 - x - 1$ is the minimal polynomial of u over $\mathbb{Q}$ (see below).

The last example is so important that we make it into a separate statement, a corollary to Proposition 2.3.5.

Corollary 2.3.7 *Under the assumptions of Proposition 2.3.5, if $f \in K[x]$ is monic irreducible and $f(u) = 0$ then $f = p$ is the minimal polynomial of u over K.*

Proof: By Proposition 2.3.5 (3), $f = ph$ for some $h \in K[x]$ (here $p = \min_{u,K}$). Since f is irreducible h must be a constant, since p isn't. Furthermore, since f and p are both monic, we must have $h = 1$, hence $f = p$. □

This discussion gives us a lot of information about the minimal polynomial of u, but all of it relies on the assumption that u is algebraic over K (or else the minimal polynomial is not defined). How can we decide whether u is algebraic or transcendental? There is one case where we can be sure, and the help again come from linear algebra.

Theorem 2.3.8 *Suppose $K \subseteq L$ is a field extension and $u \in L$. View L as a vector space over K. Then u is transcendental over K if and only if the powers of u, that is, the elements $1, u, u^2, \dots, u^k, \dots,$ are linearly independent as vectors. In particular, if $[L : K] < \infty$ then all elements of L are algebraic over K.*

Proof: Observe that linear relations among $1, u, u^2, \dots, u^k, \dots$ are in a bijective correspondence with the polynomials from the ideal I_u. Indeed, suppose $\sum_{i=1}^{\infty} a_i u^i = 0$ is a linear relation among the powers of u. If it is the trivial relation (all $a_i = 0$) then it clearly corresponds to the zero polynomial from I_u. So suppose now that the relation is nontrivial. Notice that only *finite* relations are being considered in linear algebra, so there exists n, such that $a_n \neq 0$, but $a_k = 0$ for all $k > n$. Then the polynomial corresponding to this relation is $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$. Manifestly, $f \in K[x]$ and $f(u) = 0$, so $f \in I_u$. This correspondence works in reverse as well, so it is a bijection, as claimed.

By definition, u is transcendental if and only if $I_u = \{0\}$, that is, if and only if the only linear relation among the powers $1, u, u^2, \ldots, u^k, \ldots$ is the trivial one, which means linear independence of the set of powers of u.

If $[L : K] < \infty$ then the infinitely many vectors $1, u, u^2, \ldots, u^k, \ldots$ cannot be linearly independent, so every $u \in L$ is algebraic. □

Example 2.3.9 Since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, we now know that all elements, $a + b\sqrt{2}$, of $\mathbb{Q}(\sqrt{2})$ are algebraic over $\mathbb{Q}$. We know that the minimal polynomial of $\sqrt{2}$ is $x^2 - 2$. If $a + b\sqrt{2}$ is a random element from $\mathbb{Q}(\sqrt{2})$ then it will likely have a different minimal polynomial, and it may not be so immediate to find that polynomial, but in any case, we can be sure that the minimal polynomial exists for every $a + b\sqrt{2}$. (And as we will soon see, the minimal polynomial of $a + b\sqrt{2}$ has degree at most $2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$.)

The final topic in this section is what happens with the minimal polynomial when we pass from the base field K to a larger field.

Proposition 2.3.10 *Suppose $K \subseteq M \subseteq L$ be a tower of field extensions and $u \in L$. Let $p = \min_{u,K}$ and $r = \min_{u,M}$. Then r divides p in $M[x]$. In particular, either $r = p$, or $\deg(r) < \deg(p)$ and $r \notin K[x]$.*

Proof: We first remark that, since $K \subseteq M$, we have $K[x] \subseteq M[x]$, so p is an element of $M[x]$. By Proposition 2.3.5, r divides every polynomial from $M[x]$ that evaluates to zero at $x = u$. Thus, r divides p, as $p(u) = 0$.

Suppose $r \neq p$. Since r divides p, we have $p = gr$ for some $g \in M[x]$. If g is a constant polynomial then $g = 1$, since both p and r are monic. Hence g is nonconstant, that is, $\deg(g) \geq 1$ and hence $\deg(r) < \deg(p)$. If $r \in K[x]$ then p divides r in $K[x]$, since $r(u) = 0$ (we again use Proposition 2.3.5). This means that $\deg(p) \leq \deg(r)$, a contradiction. Hence $r \notin K[x]$. □

Example 2.3.11

1. We know that the minimal polynomial of i over $\mathbb{Q}$ is $p = x^2 + 1$. If we increase the base field to $\mathbb{Q}(i)$ then the minimal polynomial becomes $r = x - i$, a polynomial of a smaller degree and with at least one coefficient not in $\mathbb{Q}$ (so that $r \notin \mathbb{Q}[x]$). We also have that $x - i$ divides $x^2 + 1$ in $\mathbb{Q}(i)[x]$.

2. If we instead increase the base field to $\mathbb{Q}(\sqrt{2})$ then $p = x^2 + 1$ remains the minimal polynomial of i over this larger base field. Hence in this case we have $r = p$.

Chapter 3

Simple extensions, splitting field

3.1 Simple extensions

Definition 3.1.1 *A field extension $K \subseteq L$ is a* simple extension *if $L = K(u)$ for some $u \in L$.*

Let $K \subseteq L$ be an arbitrary field extension, not necessarily simple. Within this extension, for every $u \in L$, the subfield $M = K(u)$ is a simple extension of K. Let ϵ_u be the the evaluation homomorphism (at $x = u$) from $K[x]$ to L, and let $I_u = \ker \epsilon_u = \{f \in K[x] \mid f(u) = 0\}$ be its kernel. Recall that u is transcendental if $I_u = \{0\}$, and u is algebraic if $I_u \neq \{0\}$. In the latter case, $I_u = (p) = \{pg \mid g \in K[x]\}$, where $p = \min_{u,K}$ is the minimal polynomial of u over K.

We will be mainly interested in the case where u is algebraic.

Proposition 3.1.2 *Suppose $K \subseteq L$ is a field extension and $M = K(u)$, where $u \in L$ is algebraic over K with the minimal polynomial p. Then $M = \operatorname{im} \epsilon_u \cong K[x]/(p)$.*

Proof: Let $M_0 = \operatorname{im} \epsilon_u$. By the first isomorphism theorem for rings, $M_0 \cong K[x]/\ker \epsilon_u = K[x]/(p)$. By Proposition 2.3.5, $p = \min_{u,K}$ is irreducible.

Now Proposition 2.1.4 implies that $I_u = (p)$ is a maximal ideal of $K[x]$, which, in turn, implies via Proposition 2.1.3 that $K[x]/I_u$ is a field. Thus, M_0 is isomorphic to a field and hence it is itself a field.

Clearly, M_0 contains K, as the elements of K are the images of the constant polynomials from $K[x]$, and M_0 contains u, as $u = \epsilon_u(x)$ (that is, u is what the polynomial x evaluates to when we substitute u for x, isn't it?!). Since M_0 contains K and u, we have $M = K(u) \subseteq M_0$. It remains to show that also $M_0 \subseteq M$. Recall that $M_0 = \operatorname{im} \epsilon_u$, that is, $M_0 = \{\epsilon_u(f) = f(u) \mid f \in K[x]\}$. Let $f \in K[x]$, say, $f = a_n x^n + a_{n-1}x^{n-1} \cdots + a_1 x + a_0$, where all $a_i \in K$. Since $K \subseteq M$ and since $u \in M$ (indeed, $u \in K(u) = M$), every summand of $f(u) = a_n u^n + a_{n-1}u^{n-1} \cdots + a_1 u + a_0$ lies in M, and hence $\epsilon_u(f) = f(u) \in M$. Thus, $M_0 \subseteq M$, and hence $M = M_0 = \operatorname{im} \epsilon_u$. □

We will exploit the fact that $K(u) = \operatorname{im} \epsilon_u$ in order to find a nice basis in $K(u)$ and determine the degree $[K(u) : K]$.

Theorem 3.1.3 *Suppose $K \subseteq L$ is a field extension and $u \in L$ is algebraic over K with the minimal polynomial p. Set $n = \deg(p)$. Then*

1. *Elements $1, u, u^2, \ldots, u^{n-1}$ form a basis of $M = K(u)$ as a vector space over K.*

2. *$[M : K] = n$.*

Proof: We first show that $1, u, u^2, \ldots, u^{n-1}$ span M. Let $v \in M$. Since $M = \operatorname{im} \epsilon_u$, there exists $f \in K[x]$, such that $v = \epsilon_u(f) = f(u)$. By the Euclidean Algorithm, there are polynomials $q, r \in K[x]$ with $\deg(r) < \deg(p)$, such that $f = qp + r$. Since $\deg(r) < \deg(p) = n$, we have $p = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ for some coefficients $a_i \in K$. Observe that $v = f(u) = q(u)p(u) + r(u) = r(u)$, since $p(u) = 0$. Thus, $v = a_{n-1}u^{n-1} + \cdots + a_1 u + a_0 = a_0 1 + a_1 u + \cdots + a_{n-1}u^{n-1}$ is a linear combination of $1, u, \ldots, u^{n-1}$.

For linear independence, suppose $a_0 1 + a_1 u + \cdots + a_{n-1}u^{n-1} = 0$ for some coefficients $a_0, \ldots, a_{n-1} \in K$. Consider the polynomial $g = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Then $g(u) = a_{n-1}u^{n-1} + \cdots + a_1 u + a_0 = 0$. This means that the minimal polynomial p of u divides g. Since $\deg(p) = n$ and $\deg(g) \leq n - 1$, we conclude that $g = 0$, that is, all $a_i = 0$.

We have shown that $1, u, \ldots, u^{n-1}$ form a basis of M over K. Since this basis consists of n vectors, $[M : K] = n$. □

Example 3.1.4

1. Since $x^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}$, Theorem 3.1.3 gives us that the familiar description of the Gaussian numbers, $\mathbb{Q}(i) = \{a + bi \,|\, a, b \in \mathbb{Q}\}$. Indeed, in this case $n = 2$ and hence 1 and i form a basis (over $\mathbb{Q}$) of $\mathbb{Q}(i)$.

2. Similarly, since $x^2 - 2$ is the minimal polynomial of $\sqrt{2}$, we see that 1 and $\sqrt{2}$ form a basis of $\mathbb{Q}(\sqrt{2})$. That is, every element of $\mathbb{Q}(\sqrt{2})$ has a unique expression as $a + b\sqrt{2}$ for $a, b \in \mathbb{Q}$ (cf. Example 1.1.4 (2)).

3. Since $x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2} = 2^{\frac{1}{3}}$, the numbers 1, $2^{\frac{1}{3}}$, and $(2^{\frac{1}{3}})^2 = 2^{\frac{2}{3}}$ form a basis of $\mathbb{Q}(\sqrt[3]{2})$. Thus, every element of $\mathbb{Q}(\sqrt[3]{2})$ can be written uniquely as $a + b2^{\frac{1}{3}} + c2^{\frac{2}{3}}$ for some $a, b, c \in \mathbb{Q}$, see Example 1.1.4 (3).

The following important result is also based on the ideas from Proposition 3.1.2, namely on the observation that $K(u) \cong K[x]/(p)$, where $p = \min_{u,K}$.

Theorem 3.1.5 (Kronecker) *Let K be a field, and $f \in K[x]$ be an arbitrary nonconstant polynomial. Then there exists a field extension $K \subseteq L$, such that L contains a root of f.*

Proof: Since $\deg(f) > 0$, f has an irreducible factor $m \in K[x]$. Consider the factor ring $L = K[x]/I$, where $I = (m)$, the ideal of $K[x]$ generated by m. Since m is irreducible, Proposition 2.1.4 implies that I is a maximal ideal of $K[x]$. Now Proposition 2.1.3 yields that L is a field. The mapping $a \mapsto a + I$ is a homomorphism from K to L. It is injective, since if a maps to the zero coset, I, then $a \in K \cap I = \{0\}$. Thus, the image of this mapping is a copy of K. We will identify every $a \in K$ with its image $a + I$ in L. In this way K becomes a subfield of L, and L becomes an extension of K.

Set $u = x + I \in L$. Assuming that $m = a_n x^n + \cdots + a_0$, we compute $m(u) = a_n(x+I)^n + a_{n-1}(x+I)^{n-1} + \cdots + a_1(x+I) + a_0 = m + I = I$. (The last equality holds since $m \in I$.) Since the coset I is the zero of L, we see that u is a root of m, hence also a root of f. □

Example 3.1.6 The polynomial $f = x^2 + x + 1 \in \mathbb{F}_2[x]$ is irreducible. (Recall, that $\mathbb{F}_2$ is the finite field of order two.) Indeed, neither 0, nor 1 is a root of f, and hence f is irreducible by Proposition 2.2.3. Let $F = \mathbb{F}_2[x]/(f)$. Then F is a field, an extension of $\mathbb{F}_2$. Let ζ be a root of f in F (we can take $\zeta = x + (f) \in F$). Then f is the minimal polynomial of ζ over $\mathbb{F}_2$. This means that $[F : \mathbb{F}_2] = \deg(f) = 2$ and furthermore 1 and ζ form a basis of F over $\mathbb{F}_2$. Hence every element of F can be written uniquely as $a + b\zeta$, $a, b \in \mathbb{F}_2$. Since there are two choices for each of a and b, the size of F is four. Thus, we have constructed a finite field of size four. Our description of F is completely explicit and it allows us to perform efficiently all operations in F.

Similarly, $g = x^3+x+1 \in \mathbb{F}_2[x]$ is irreducible, which means that $\mathbb{F}_2[x]/(g)$ is a field, namely, an extension of $\mathbb{F}_2$ of degree three. The elements 1, ξ, ξ^2, where $\xi = x + (g)$, form a basis of this field over $\mathbb{F}_2$, and hence the size of this new field is $2^3 = 8$.

Similarly, if $f \in \mathbb{F}_p[x]$, p a prime, is an irreducible polynomial of degree k then $\mathbb{F}_{p^k} = \mathbb{F}_p/(f)$ is a finite field of size $q = p^k$. It can be shown that irreducible polynomials exist for all primes p and all degrees k. Thus, for all prime powers p^k, finite fields of size p^k exist.

3.2 Polynomial rewriting, uniqueness of the simple extension

There was a bit of “cheating” in the proof of Kronecker’s Theorem, and before we have moved too far ahead with our course, let us clarify the details of what we actually did. The “cheating” occurred, when we identified elements $a \in K$ with the corresponding elements of L, namely, with the cosets $a + I$. By doing this, we hid the important fact that L is in fact an extension of the field $K' = \{a + I \mid a \in K\}$, isomorphic to K, and not of K itself. If so, how can we then plug $x = u$ into $m = a_n x^n + \cdots + a_0$? The coefficients a_i being in

K, while u^i being in L, how can we multiply one with the other? The answer is, we multiply u^i not with a_i, but rather with the corresponding coset a_i+I, which is in L. That is, in place of m, we plug $x = u$ into the polynomial $m' = (a_n+I)x^n+(a_{n-1}+I)x^{n-1}+\cdots+(a_1+I)x+(a_0+I) \in K'[x]$, which we have to identify with m, once we identify K with K'. Thus, the identification of K with K' forces also the identification of $K[x]$ with $K'[x]$.

The identification in the proof of Theorem 3.1.5 is an instance of the general concept of field isomomorphism. Just like an identification of two fields forces an identification of polynomials defined over the two fields, an arbitrary field isomorphism induces an isomorphism between the corresponding rings of polynomials.

Definition 3.2.1 *Suppose K and K' are isomorphic fields and $\theta : K \longrightarrow K'$ is an isomomorphism. The* polynomial rewriting *associated with θ is the mapping $\bar{\theta} : K[x] \longrightarrow K'[x]$ defined by*

$$\bar{\theta}(a_nx^n + \cdots + a_0) = \theta(a_n)x^n + \cdots + \theta(a_0).$$

Proposition 3.2.2 *For fields K, K' and an isomorphism $\theta : K \longrightarrow K'$, let $\bar{\theta} : K[x] \longrightarrow K'[x]$ be the corresponding polynomial rewriting. Then the following hold:*

1. *$\bar{\theta}$ is an isomorphism of rings;*

2. *$\bar{\theta}|_K = \theta$ (that is, $\bar{\theta}$ extends θ) and $\bar{\theta}(x) = x$.*

3. *The inverse of $\bar{\theta}$ is $\overline{\theta^{-1}}$.*

4. *$\bar{\theta}$ sends ideals to ideals; namely, the ideal (f) of $K[x]$ is mapped onto the ideal $(\bar{\theta}(f))$ of $K'[x]$.*

5. *If $f \in K[x]$ is irreducible then $\bar{\theta}(f)$ is irreducible in $K'[x]$; equivalently, $\bar{\theta}$ sends maximal ideals of $K[x]$ to maximal ideals of $K'[x]$.*

Proof: Claims 2 and 3 follow directly from the definition of $\bar{\theta}$. In particular, θ is bijective. The check that $\bar{\theta}$ preserves addition and multiplication is left to the reader. (This gives claim 1.) Since $\bar{\theta}$ is an isomorphism of rings, it sends ideals to ideals. Recall that $K[x]$ is a principal ideal domain (Theorem 2.1.2). Suppose $I = (p) = pK[x]$, for $p \in K[x]$, is an ideal of $K[x]$. Then $\bar{\theta}(I) = \bar{\theta}(pK[x]) = \bar{\theta}(p)\bar{\theta}(K[x]) = \bar{\theta}(p)K'[x] = (\bar{\theta}(p))$, proving claim 4.

Suppose I is a maximal ideal of $K[x]$ and suppose $I' = \bar{\theta}(I)$ is not maximal in $K'[x]$. Then I' is contained in a larger ideal J' of $K'[x]$. Let $\phi = \theta^{-1}$ and set $J = \bar{\phi}(J')$. By claim 3 applied to ϕ (in place of θ), J is an ideal of $K[x]$ and, clearly, $J \supset I$. Hence I is not maximal. The contradiction yields the second part of claim 5. Since $f \in K[x]$ is irreducible if and only if (f) is maximal (and the same applies to polynomials in $K'[x]$), we conclude that f is irreducible in $K[x]$ if and only if $\bar{\theta}(f)$ is irreducible in $K'[x]$. □

We also remark that $\bar{\theta}$ sends monic polynomials again to monic polynomials.

The rewriting isomorphism $\bar{\theta}$, induced by θ, induces in its turn isomorphisms on the corresponding factor rings of $K[x]$ and $K'[x]$.

Proposition 3.2.3 *Suppose K, K', θ and $\bar{\theta}$ be as above. Then for every $f \in K[x]$, $\bar{\theta}$ induces a ring isomorphism $\phi_f : K[x]/(f) \longrightarrow K'[x]/(\bar{\theta}(f))$. In particular, if f is irreducible then ϕ_f is a field isomorphism between the fields $K[x]/(f)$ and $K'[x]/(\bar{\theta}(f))$.*

Proof: Let $I = (f)$ and $I' = \bar{\theta}(I) = (\bar{\theta}(f))$. Every element of the factor ring $K[x]/I$ is a coset $g+I$. Its image under $\bar{\theta}$ is $\bar{\theta}(g+I) = \bar{\theta}(g)+\bar{\theta}(I) = \bar{\theta}(g)+I'$, a coset of I' and hence an element of $F'[x]/I'$. This means that $\bar{\theta}$ indeed induces a mapping $\phi_f : K[x]/I \longrightarrow K'[x]/I'$ defined by $g + I \mapsto \bar{\theta}(g) + I'$. Since $\bar{\theta}$ is bijective, ϕ_f is bijective, too. The check that ϕ_f preserves addition and multiplication is left to the reader.

The last claim corresponds to the case where I and I' are maximal in $K[x]$ and $K'[x]$, respectively. □

We now return to the simple extensions.

Theorem 3.2.4 *Suppose $K \subseteq L$ and $K' \subseteq L'$ are two field extensions and suppose $\theta : K \longrightarrow K'$ is an isomorphism. Let $u \in L$ and $u' \in L'$ be algebraic over K and K' with minimal polynomials p and p', respectively. Then θ extends to an isomorphism $\phi : K(u) \longrightarrow K'(u')$ sending u to u' if and only if $p' = \bar{\theta}(p)$. Furthermore, such an extension, if exists, is unique.*

Proof: Recall that ϕ is an extension of θ if $\phi|_K = \theta$. Suppose an extension ϕ sending u to u' exists. Then $0 = \phi(0) = \phi(p(u)) = \phi(a_n u^n + \cdots + a_0) = \phi(a_n)\phi(u)^n + \cdots + \phi(a_0) = \theta(a_n)(u')^n + \cdots + \theta(a_0) = \bar{\theta}(p)(u')$. This means that u' is a root of $\bar{\theta}(p)$. Since p is irreducible and monic, $\bar{\theta}(p)$ is also irreducible and monic (cf. Proposition 3.2.2 and the remark after it). According to Corollary 2.3.7, this means that $\bar{\theta}(p)$ is the minimal polynomial of u', that is, $\bar{\theta}(p) = p'$.

Reversely, suppose $\bar{\theta}(p) = p'$. According to Proposition 3.1.2, $K(u) = \operatorname{im} \epsilon_u$, where ϵ_u is the evaluation homomorphism from $K[x]$ to L. By the first isomorphism theorem, this leads to the isomorphism $\alpha : K[x]/(p) \longrightarrow K(u)$, since $(p) = I_u = \ker \epsilon_u$. Note that $\alpha(a + (p)) = a$ for all $a \in K$ and $\alpha(x + (p)) = u$. Similarly, there is an isomorphism $\alpha' : K'[x]/(p') \longrightarrow K'(u')$, such that $\alpha'(a + (p')) = a$ for all $a \in K'$ and $\alpha'(x + (p')) = u'$. Furthermore, according to Proposition 3.2.3, polynomial rewriting $\bar{\theta}$ induces an isomorphism $\phi_p : K[x]/(p) \longrightarrow K'[x]/(p')$ (here we use that $\bar{\theta}(p) = p'$). Observe that $\phi_p(a + (p)) = \bar{\theta}(a) + (p') = \theta(a) + (p')$ for all $a \in F$, and $\phi_p(x + (p)) = \bar{\theta}(x) + (p') = x + (p')$.

We now put everything together: the composition $\phi = \alpha'\phi_p\alpha^{-1}$ is an isomorphism from $K(u)$ onto $K'(u')$ and, furthermore, $\alpha'\phi_p\alpha^{-1}(a) = \alpha'\phi_p(a + (p)) = \alpha'(\theta(a) + (p')) = \theta(a)$ for all $a \in K$ (so ϕ_p is an extension of θ) and $\alpha'\phi_p\alpha^{-1}(u) = \alpha'\phi_p(x + (p)) = \alpha'(x + (p')) = u'$. Thus, ϕ is as claimed.

To establish the uniqueness of ϕ, suppose ψ is a second extension of θ and $\psi(u) = u'$. By Proposition 3.1.2, $K(u) = \operatorname{im} \epsilon_u$ and so every $v \in K(u)$ can be written as $v = a_n u^n + \cdots + a_0$ for some $a_n, \ldots, a_0 \in K$. Then $\phi(v) = \phi(a_n u^n + \cdots + a_0) = \theta(a_n)(u')^n + \cdots + \theta(a_0) = \psi(a_n u^n + \cdots + a_0) = \psi(v)$. Thus, $\psi = \phi$. □

As a corollary to this important theorem, we obtain the following result on the uniqueness of simple extension corresponding to the given *irreducible* polynomial. This result complements Kronecker's Theorem.

Corollary 3.2.5 *Suppose $K \subseteq L$ is a field extension and suppose $u, u' \in L$ are two roots of the same irreducible polynomial f. Then $K(u)$ and $K(u')$ are isomorphic; namely, there is an isomorphism $\phi : K(u) \longrightarrow K(u')$, such that $\phi|_K = id$ and $\phi(u) = u'$.*

Proof: Since u and u' are roots of f and f is irreducible, elements u and u' have the same minimal polynomial, $\frac{1}{a}f$, where a is the leading coefficient of

f. Now apply Theorem 3.2.4 with $K' = K$, $L' = L$, and $\theta = id$. Clearly, $\bar{\theta} = id$ and so $\bar{\theta}(p) = p$. □

Example 3.2.6 1. Consider the Gaussian numbers $\mathbb{Q}(i)$. We have that $\mathbb{Q}(i) = \mathbb{Q}(-i)$ and, clearly, i and $-i$ have the same minimal polynomial $x^2 + 1$. Thus, there must exist an automorphism (isomorphism onto itself) of $\mathbb{Q}(i)$ sending i to $-i$. And indeed, such an automorphism is induced by complex conjugation.

2. Similarly, $\sqrt{2}$ and $-\sqrt{2}$ have the same minimal polynomial $x^2 - 2$ and hence $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$ has an automorphism sending $\sqrt{2}$ to $-\sqrt{2}$. Since an arbitrary element of $\mathbb{Q}(\sqrt{2})$ can be written as $a + b\sqrt{2}$ for $a, b \in \mathbb{Q}$, we conclude that this automorphism acts as follows: $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ for all $a, b \in \mathbb{Q}$.

3. A slightly more complicated example: The three roots of $x^3 - 2$ are $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta$, and $\sqrt[3]{2}\zeta^2$, where $\zeta = e^{\frac{2\pi i}{3}}$ is the primitive cubic root of unity. By Corollary 3.2.5, there is an isomorphism from $\mathbb{Q}(\sqrt[3]{2})$ onto $\mathbb{Q}(\sqrt[3]{2}\zeta)$, even though the first field is fully real and the second one is not.

4. Both i and $\sqrt{2}$ are roots of $f = x^4 - x^2 - 2 = (x^2 + 1)(x^2 - 2)$. However, there is no isomorphism from $\mathbb{Q}(i)$ onto $\mathbb{Q}(\sqrt{2})$. Indeed, if ϕ is such an isomorphism then $\phi(i) \in \mathbb{Q}(\sqrt{2})$ is a root of $x^2 + 1$; a contradiction, since $x^2 + 1$ has no root in $\mathbb{Q}(\sqrt{2})$. This shows that the analog of Corollary 3.2.5 for arbitrary polynomials f is false.

3.3 Splitting field

Definition 3.3.1 *Let K be a field, $f \in K[X]$, and L be an extension of K. Then we say that f* splits *in L if f factorizes into linear factors over L; that is, $f = a(x - u_1)^{s_1} \cdots (x - u_k)^{s_k}$ for some $a \in K$, $u_1, \ldots, u_k \in L$, and positive* *integers $s_1, \ldots, s_k$. Moreover, L is a* splitting field *for f if f splits in L and L is generated by K and the elements $u_1, \ldots, u_k$.*

Notice that $u_1, \ldots, u_k$ are roots (zeros) of f and, in fact, they form a *full* set of roots, meaning that in any extension of L the set of roots of f will always be restricted to $\{u_1, \ldots, u_k\}$. Indeed, if L' is an extension of L and if $u \in L$ then, after plugging $x = u$ into $f = a(x - u_1)^{s_1} \cdots (x - u_k)^{s_k}$, we see that u is a root of f if and only if one of the factors $u - u_i$ is zero, that is, $u = u_i$.

We also remark that a in $f = a(x - u_1)^{s_1} \cdots (x - u_k)^{s_k}$ is simply the leading coefficient of f and so it is independent of L. The integers $s_1, \ldots, s_k$ are the *multiplicities* of the roots $u_1, \ldots, u_k$.

If $K = \mathbb{Q}$ then every polynomial $f \in K[x]$ splits in $\mathbb{C}$. Thus, a splitting field for f can be constructed by adding to $\mathbb{Q}$ all complex roots of f. Here are some examples of this sort.

Example 3.3.2 1. Let $f = X^3 - 2 \in \mathbb{Q}[x]$. Then the roots of f are $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta$, and $\sqrt[3]{2}\zeta^2$, where $\zeta = e^{\frac{2\pi i}{3}}$. Clearly, $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2)$ is a splitting field for f. Indeed, f splits over L as follows: $f = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\zeta)(x - \sqrt[3]{2}\zeta^2)$.

We can also write $L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$. With this expression, it is easier to find the degree $[L : \mathbb{Q}]$. By the Tower Law $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$. Clearly, the minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$ (since this monic polynomial is irreducible; cf. Proposition 2.2.3). Thus, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ by Theorem 3.1.3. Since $L = M(\zeta)$, where $M = \mathbb{Q}(\sqrt[3]{2})$, it remains to determine the minimal polynomial of ζ over M. We claim that the minimal polynomial of ζ over M (as well as over $\mathbb{Q}$) is $\frac{x^3-1}{x-1} = x^2 + x + 1$. Indeed, ζ is a root of this polynomial, so $\min_{\zeta,M}$ must divide $x^2 + x + 1$. On the other hand, ζ is not real, so $\zeta \notin M$ and hence $\min_{\zeta,M}$ cannot have degree less than two. Thus, $x^2 + x + 1 = \min_{\zeta,M}$ and hence $[L : M] = [L : \mathbb{Q}(\sqrt[3]{2})] = 2$. This yields $[L : \mathbb{Q}] = 6$.

2. Let $f = x^n - 1$ and let $\zeta = e^{\frac{2\pi i}{n}}$ be the primitive complex nth root of unity. Then the roots of f are $1, \zeta, \ldots, \zeta^{n-1}$. Thus, $\mathbb{Q}(\zeta, \ldots, \zeta^{n-1}) = \mathbb{Q}(\zeta)$ is a splitting field for f. For example, if $n = 8$, then $f = x^8 - 1 = (x-1)(x+1)(x^2+1)(x^4+1)$, where all factors are irreducible over $\mathbb{Q}$. Since ζ is not a root of either of the first three factors, it must be a root of $x^4 + 1$, which is, therefore, the minimal polynomial of ζ. Thus, for $n = 8$, the degree of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ is four.

3. If $f = x^4 + 1$ then its roots are $\zeta = e^{\frac{\pi i}{4}}$, ζ^3, ζ^5, and ζ^7. Thus, the same $\mathbb{Q}(\zeta)$ is also a splitting field for $x^4 + 1$.

We have already seen that the splitting field can be constructed inside $\mathbb{C}$ when $K = \mathbb{Q}$ (or, in fact, any subfield of $\mathbb{C}$). The following theorem contains the general result for splitting fields.

Theorem 3.3.3 *Let K be a field and $f \in K[x]$. Then there exists a splitting field for f over K.*

Proof: We use induction on $\deg(f) = n$. If $n = 1$ then f is linear and so it already splits in K, and so K itself is a splitting field for f. Now suppose that $n > 1$. By Theorem 3.1.5, there is an extension field M containing a root u of f. Consider $K(u)$. Now $f \in K[x] \subseteq K(u)[x]$, and as $f(u) = 0$, there exists a polynomial $g \in K(u)[x]$, such that $f = (x-u)g$. Now $\deg(g) < n$, and so by induction we have a splitting field L for g over $K(u)$. Since g splits in L, so does f. Also, L is generated by $K(u)$ and the roots of g. Hence L is generated by K, u, and the roots of g, and so L is a splitting field for f over K. □

There is a subtlety in this proof: mid-way through we change from one base field to another, and use the inductive argument on this new field. This is perfectly allowable, since we are proving simultaneously by induction that *all polynomials* f over *all fields* K have splitting fields. We have to assume this when we take our inductive step.

Next we prove the uniqueness of the splitting field. Note that every splitting field L is a finite extension of the base field K. Indeed, if $\deg(f) = n$ then f has at most n roots, and so L can be obtained as a result of a series of at most n simple extensions. Furthermore, at each step the minimal polynomial divides f and so the total degree $[L : K]$ does not exceed n^n (a more careful estimate yields the bound $[L : K] \leq n!$).

Theorem 3.3.4 *Let K and K' be isomorphic fields and let $\theta : K \to K'$ be an isomorphism. Let $\bar{\theta}$ be the polynomial rewriting induced by θ. Suppose that $f \in K[x]$ and let $f' = \bar{\theta}(f)$. Let L and L' be splitting fields of f and f' over K and K', respectively. Then θ extends to an isomorphism from L onto L'.*

Proof: We use induction on the degree $[L : K]$ (which is finite by the remark above). Let $[L : K] = m$. If $m = 1$, then $L = K$ and so f splits over K. That is, $f = a(x-u_1)^{s_1} \cdots (x-u_k)^{s_k}$ for some $a, u_1, \ldots, u_k \in K$ and positive integers $s_1, \ldots, s_k$. Hence $f' = \bar{\theta}(f) = \bar{\theta}(a)\bar{\theta}(x-u_1)^{s_1} \cdots \bar{\theta}(x-u_k)^{s_k} = \theta(a)(x-\theta(u_1))^{s_1} \cdots (x-\theta(u_k))^{s_k}$ also splits over K'. Thus, $L' = K'$ and there is nothing to prove.

Now suppose that $n > 1$ and that the result holds for all extensions of lesser degree. Let $u \in L$ be a root of f with $u \notin K$. Let $p \in K[x]$ be the minimal polynomial of u over K. Since $f(u) = 0$, p divides f in $K[x]$, thus, there exists $g \in K[x]$ such that $f = pg$.

Let $p' = \bar{\theta}(p)$ and $g' = \bar{\theta}(g)$. By Proposition 3.2.2, we have $f' = p'g'$. Since f' splits in L', L' contains a root of p', say u'. By Proposition 3.2.2, p' is irreducible. Also, p' is monic, since p is monic. Thus, p' is the minimal polynomial of u'. Now Theorem 3.2.4 gives an isomorphism $\phi : K(u) \to K'(u')$ extending θ and sending u to u'. By the Tower Law, we have $[L : K] = [L : K(u)][K(u) : K]$. So $[L : K(u)] < [L : K]$. We know that $f \in K(u)[x]$ and $f' = \bar{\theta}(f) = \bar{\phi}(f) \in K'(u')[x]$. Now L and L' are splitting fields for f and f' over $K(u)$ and $K'(u')$, respectively. By induction, there exists an isomorphism from L onto L' extending ϕ (and hence also extending θ). □

The important case is when $K' = K$ and $\theta = id$.

Corollary 3.3.5 *Let K be a field and $f \in K[x]$. Then any two splitting fields of f over K are isomorphic and the isomorphism can be chosen so that its restriction to K is the identity mapping.* □

Thus, splitting fields are unique up to isomorphism. So we can refer to *the* splitting field of f over K.

Chapter 4

Galois groups and normal extensions

4.1 Prime subfield, characteristic

Suppose K is a field. Let $\rho : \mathbb{Z} \to K$ be the mapping defined as follows:

$$\rho(n) = \begin{cases} 0, & \text{if } n = 0; \\ \underbrace{1 + \cdots + 1}_{n}, & \text{if } n > 0; \\ \underbrace{-1 - \cdots - 1}_{|n|}, & \text{if } n < 0. \end{cases}$$

Proposition 4.1.1 *The mapping ρ is a ring homomorphism.* □

We will now discuss the kernel and the image of this homomorphism.

Recall that a *zero divisor* in a commutative ring R is an element $0 \neq a \in R$ such that there exists $0 \neq b \in R$ with $ab = 0$. An ideal $I \subseteq R$ is *prime* if the factor ring R/I has no zero divisors.

Proposition 4.1.2 *The subring $\operatorname{im} \rho$ of K has no zero divisors, and hence $\ker \rho$ is a prime ideal of $\mathbb{Z}$.*

Proof: K contains no zero divisors, since every nonzero element of K is invertible. Hence $\operatorname{im} \rho \cong \mathbb{Z}/\ker \rho$ has no zero divisors. □

Proposition 4.1.3 *An ideal I of $\mathbb{Z}$ is prime if and only if either $I = \{0\}$, or $I = (p)$ for some prime number p.* □

Combining Propositions 4.1.2 and 4.1.3 together, we conclude that either $\ker \rho = \{0\}$, or $\ker \rho = (p)$ for some prime p.

Definition 4.1.4 *If* $\ker \rho = \{0\}$ *then we say that K has* zero characteristic, *and we write* $\mathrm{char}(K) = 0$. *Similarly, if* $\ker \rho = (p)$ *then we say that K has* positive characteristic p, *and write* $\mathrm{char}(K) = p$.

Proposition 4.1.5 *Every field K contains a unique smallest subfield K_0. If K has a positive characteristic p then $K_0 = \mathrm{im}\,\rho \cong \mathbb{F}_p$. If* $\mathrm{char} K = 0$ *then $K_0 \cong \mathbb{Q}$ is the field of fractions of* $\mathrm{im}\,\rho \cong \mathbb{Z}$.

Proof: If M is a subfield of K then $1 \in M$ and hence $\rho(n) \in M$ for all $n \in \mathbb{Z}$. Thus, $\mathrm{im}\,\rho$ is contained in M, and hence in every subfield of K. If $\mathrm{char}(K) = p$ then $\mathrm{im}\,\rho \cong \mathbb{Z}/\ker \rho = \mathbb{Z}/(p) = \mathbb{F}_p$. Therefore, $\mathrm{im}\,\rho$ is itself a subfield, and it is the unique smallest subfield. Thus, $K_0 = \mathrm{im}\,\rho \cong \mathbb{F}_p$. Now suppose $\mathrm{char}(K) = 0$. By definition, this means that $\ker \rho = \{0\}$, that is, ρ is injective. Thus, in this case $\mathrm{im}\,\rho \cong \mathbb{Z}$. Since $\mathrm{im}\,\rho$ is contained in every subfield of K, its field of fractions, $\{\frac{a}{b} \,|\, a, b \in \mathrm{im}\,\rho, b \neq 0\}$, is also contained in every subfield of K, that is, the field of fractions of $\mathrm{im}\,\rho$ is F_0, the unique smallest subfield of K. Since $\mathrm{im}\,\rho \cong \mathbb{Z}$, we have that $K_0 \cong \mathbb{Q}$. □

Definition 4.1.6 *The unique smallest subfield of K is called the* prime subfield *of K.*

We repeat that the prime subfield is isomorphic to $\mathbb{F}_p$ if $\mathrm{char}(K) = p > 0$, and $\mathbb{Q}$ if $\mathrm{char}(K) = 0$. The proof of the following fact is left to the reader.

Proposition 4.1.7 *If $K \subseteq L$ is a field extension then K and L have the same prime subfield and hence the same characteristic.* □

Example 4.1.8

1. $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields of zero characteristic. It follows from Proposition 4.1.7 that all subfields of $\mathbb{C}$ (which appear in a wide majority of our examples) are of zero characteristic.

2. On the other hand, if K is a finite field then K cannot contain a copy of $\mathbb{Q}$ and hence K has characteristic p for some prime p. Let $K_0 \cong \mathbb{F}_p$ be the prime subfield of K and let $n = [K : K_0]$. Choose a basis $u_1, \ldots, u_n$ for K over K_0 and observe that every element of K can be expressed uniquely as $u = a_1u_1 + \cdots + a_nu_n$ for $a_1, \ldots, a_n \in K_0$. Thus, the number of elements in K coincides with the number of ways the coefficients of the linear combination can be chosen, that is, with q^n. We have shown that the size of every finite field K is a prime power p^n, where $p = \text{char}(K)$ and n is the degree of K over its prime subfield.

3. Since K is a subfield of the ring $K[x_1, \ldots, x_n]$, it is also a subfield of its field of fractions, $K(x_1, \ldots, x_n)$. Thus, K and $K(x_1, \ldots, x_n)$ have the same characteristic. This leads to more examples both in characteristic zero and in the positive characteristic. In particular, this gives infinite fields of positive characteristic.

4.2 Galois groups

Recall that an *automorphism* of a field L is an isomorphism from L to L. The set of all automorphisms of a field L is denoted by $\text{Aut}(L)$. We leave it to the reader to verify that $\text{Aut}(L)$ is a group with respect to the operation of multiplication given by composition.

Definition 4.2.1 *Let $K \subseteq L$ be a field extension. The* Galois group *of this extension, denoted by* $\text{Gal}(L/K)$*, consists of all automorphisms α of L, satisfying $\alpha(k) = k$ for all $k \in K$ (that is, $\alpha|_K = id$).*

The group $\text{Gal}(L/K)$ is a subgroup of $\text{Aut}(L)$, the elementwise stabilizer in $\text{Aut}(L)$ of K. Note that $\alpha \in \text{Aut}(L)$, such that $\alpha|_K = id$, is called a *K-automorphism* of L. Thus, $\text{Gal}(L/K)$ consists of all K-automorphisms of L.

The proof of the following basic properties of Galois groups is left as an exercise.

Proposition 4.2.2 *Let L be a field.*

1. $\mathrm{Gal}(L/L) = 1$.

2. *If L_0 denotes the prime subfield of L then* $\mathrm{Gal}(L/L_0) = \mathrm{Aut}(L)$.

3. *If $K \subseteq M$ are two subfields of L then* $\mathrm{Gal}(L/M) \leq \mathrm{Gal}(L/K)$. □

Example 4.2.3

1. The complex conjugation is an $\mathbb{R}$-automorphism of $\mathbb{C}$ and hence an element of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. We will soon see that it is the only nonidentity element of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ (that is, $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| = 2$).

2. It can be shown that $\mathbb{C}$ has infinitely many automorphisms. Since $\mathbb{Q}$ is the prime subfield of $\mathbb{C}$, we conclude that $\mathrm{Gal}(\mathbb{C}/\mathbb{Q}) = \mathrm{Aut}(\mathbb{C})$ is an infinite group.

3. It can also be shown that $\mathbb{R}$ has *no* nonidentity automorphisms and so $\mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = 1$.

4. The automorphism $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ (cf. Example 3.2.6 (2)) is a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt{2})$. Notice that $\mathbb{Q}$ is the prime subfield of $\mathbb{Q}(\sqrt{2})$ and so every automorphism of $\mathbb{Q}(\sqrt{2})$ is a $\mathbb{Q}$-automorphism.

We will now study the action of $\mathrm{Gal}(L/K)$ on the elements of L.

Proposition 4.2.4 *Suppose $K \subseteq L$ is a field extension and $f \in K[x]$. Then* $\mathrm{Gal}(L/K)$ *acts on the set of roots of f in L.*

Proof: Clearly, $G = \mathrm{Gal}(L/K)$ acts on the set of elements of L. Thus, in order to establish the claim, we need to show that G leaves $R = \{a \in L \mid f(a) = 0\}$ invariant.

Let $\alpha \in G$ and suppose $u \in R$. Then $f(u) = 0$ and hence $0 = \alpha(0) = \alpha(f(u))$. Suppose $f = a_n x^n + \cdots + a_0$. Since the coefficients of f are in K and hence they are fixed (left unchanged) by α, we have $0 = \alpha(f(a)) = \alpha(a_n u^n + \cdots + a_0) = \alpha(a_n)(\alpha(u))^n + \cdots + \alpha(a_0) = a_n(\alpha(u))^n + \cdots + a_0 = f(\alpha(a))$.

Thus, $\alpha(u)$ is again a root of f. That is, $\alpha(u) \in R$ for all $u \in R$ and all $\alpha \in G$. □

Let us now look at the action of $G = \mathrm{Gal}(L/K)$ on L from a different angle. Suppose $u \in L$. Recall that the *orbit* of u under the action of G is the set $\{\alpha(u) \mid \alpha \in G\}$. What can we say about this orbit? How big can it be?

Corollary 4.2.5 *Suppose $K \subseteq L$ is a field extension, $G = \mathrm{Gal}(L/K)$, and $u \in L$. Then the orbit of u under the action of G is contained in the set of roots of the minimal polynomial $p = \min_{u,K}$. In particular, the size of the orbit is at most $k = \deg(p) = [K(u) : K]$.*

Proof: Applying Proposition 4.2.4 with $f = p$, we see that the set of roots of p is invariant under the action of G. Since u is a root of p, the entire orbit of u must be contained in the set of roots of p.

By Corollary 2.2.2, p has no more than $\deg(p)$ roots, so the last claim follows as well. □

When a group acts on a set, a lot of important information about the action is contained in the stabilizers of particular elements. Recall that $G_{u_1,\ldots,u_k}$ denotes the (elementwise) stabilizer in G of the elements $u_1, \ldots, u_k$.

Proposition 4.2.6 *Suppose $K \subseteq L$ is a field extension and $G = \mathrm{Gal}(L/K)$. If $u_1, \ldots, u_k \in L$ then $G_{u_1,\ldots,u_k} = \mathrm{Gal}(L/K(u_1, \ldots, u_k))$.*

Proof: Clearly (cf. Proppposition 4.2.2), $H = \mathrm{Gal}(L/K(u_1, \ldots, u_k))$ is a subgroup of $G = \mathrm{Gal}(L/K)$ and, furthermore, H stabilizes every element u_i, since $u_i \in K(u_1, \ldots, u_k)$. Thus, $H \leq G_{u_1,\ldots,u_k}$.

For the reverse inclusion, we will first deal with the case $k = 1$. Let $u = u_1$. Let $\alpha \in G_u$. Then α acts trivially on K (since all elements of $G = \mathrm{Gal}(L/K)$ do) and α fixes (stabilizes) u. By Proposition 3.1.2, $K(u) = \mathrm{im}\,\epsilon_u$, where ϵ_u is the evaluation map at $x = u$. This means that every $v = \epsilon_u(g) = g(u)$ for some $g \in K[x]$. Assuming $g = a_n x^n + \cdots + a_0$, we obtain $v = a_n u^n + \cdots + a_0$. Since $a_1, \ldots, a_n \in K$, the automorphism α fixes every term on the right and therefore α fixes v. Thus, α fixes every $v \in K(u)$, that is, $\alpha \in \mathrm{Gal}(L/K(u))$, yielding $G_u \leq H = \mathrm{Gal}(L/K(u))$.

Now, let us do the case of arbitrary k. We will use induction. The case $k = 1$ supplies the basis of induction. If $k > 1$, let $\alpha \in G_{u_1,\ldots,u_k}$ and set

$K' = K(u_1, \ldots, u_{k-1})$. By induction, α fixes every element of K', hence $\alpha \in G' := \mathrm{Gal}(L/K')$. Furthermore, $\alpha \in G'_{u_k}$. Hence, by the above (case $k = 1$), α fixes every element of $K'(u_k)$. However, $K'(u_k) = K(u_1, \ldots, u_{k-1}, u_k)$. Thus, $\alpha \in H$, yielding the reverse inclusion $G_{u_1,\ldots,u_k} \leq H$. □

An important case is where $u_1, \ldots, u_k$ generate the entire L.

Corollary 4.2.7 *Suppose $K \subset L$ is a field extension, $G = \mathrm{Gal}(L/K)$ and $L = K(u_1, \ldots, u_k)$ for some $u_1, \ldots, u_k \in L$. Then $G_{u_1,\ldots,u_k} = 1$.*

Proof: According to Proposition 4.2.6, $G_{u_1,\ldots,u_k} = \mathrm{Gal}(L/K(u_1, \ldots, u_k)) = \mathrm{Gal}(L/L) = 1$ (cf. Proposition 4.2.2). □

When a group G acts on a set R, the action of each $\alpha \in G$ is a permutation $\sigma_\alpha \in \mathrm{Sym}(R)$. The mapping $\alpha \mapsto \sigma_\alpha$ is a homomorphism from G to $\mathrm{Sym}(R)$. We say that the action of G on R is *faithful* if the associated homomorphism $G \to \mathrm{Sym}(R)$ is injective, that is, the kernel of this homomorphism is trivial, that is, the identity element is the only element of G that fixes all elements of R. If the action of G is faithful then G is isomorphic to its image in $\mathrm{Sym}(R)$ (this follows from the first isomorphism theorem).

The following is the main result of this section.

Proposition 4.2.8 *Let K be a field, and $f \in K[x]$. Let L be the splitting field for f over K. Let R be the set of roots of f in L. Then $G = \mathrm{Gal}(L/K)$ acts faithfully on R. In particular, G is isomorphic to a subgroup of the (finite) group $\mathrm{Sym}(R)$.*

Proof: The claim that G acts on R follows from Proposition 4.2.4. The fact that this action is faithful follows from Corollary 4.2.7, since $L = K(R)$. □

Definition 4.2.9 *Suppose K is a field and $f \in K[x]$. The* Galois group *of f is the group $\mathrm{Gal}(L/K)$, where L is the splitting field for f over K.*

Example 4.2.10 1. Consider the extension $\mathbb{R} \subseteq \mathbb{C}$. Note that $\mathbb{C} = \mathbb{R}(i)$. Since $\pm i \in \mathbb{C}$ are the roots of the polynomial $x^2 + 1$, we conclude that $\mathbb{C}$ is the splitting field for $x^2 + 1$ over $\mathbb{R}$. Let $R = \{i, -i\}$. By Proposition 4.2.8, there is an injective homomorphism $\theta : \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to$

$\mathrm{Sym}(R) \cong S_2$. So $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| \leq 2$. Note that the complex conjugation is an element of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. This means that $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong S_2$ has order two. Note also that this means that the complex conjugation is the only nontrivial $\mathbb{R}$-autmomorphism of $\mathbb{C}$.

2. Similarly, $\mathbb{Q}(\sqrt{2})$ is the splitting field of $f = x^2 - 2$ and so the Galois group of f, $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, acts faithfully on $R = \{\sqrt{2}, -\sqrt{2}\}$. We have seen that the mapping $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is a nontrivial $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt{2})$. Therefore, $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong S_2$.

3. The splitting field of the polynomial $f = x^3 - 2$ coincides with $L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$, where $\zeta = e^{\frac{2\pi i}{3}}$ is the primitive cubic root of one. By Proposition 4.2.8, we know that $G = \mathrm{Gal}(L/\mathbb{Q})$ acts faithfully on $R = \{\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2\}$, the set of roots of f. Thus, G is isomorphic to a subgroup of S_3. Which one? At the moment we only know that G contains the automorphism of L induced by complex conjugation (it fixes the real root $\sqrt[3]{2}$, and interchanges the two complex roots). So $|G| \geq 2$.

4.3 Normal extensions

In this section we introduce normal field extensions and study their properties. In a sense, normal extensions are not new objects for us, because normal finite extensions are exactly the extensions $K \subseteq L$, where L is the splitting field of some polynomial from $K[x]$. Thus, normal extensions have to do with splitting fields.

We can take this as a temporary definitions of normal extensions. Later in this section we give a different definition, that also applies to infinite extensions, and we will show the equivalence of that new definition and the current definition, when the extension is finite.

Proposition 4.3.1 *Suppose $K \subseteq L \subseteq M$ is a tower of field extensions,* *where L is the splitting field over K of some polynomial $f \in K[x]$. Then $\alpha(L) = L$ for all $\alpha \in \mathrm{Gal}(M/K)$.*

Proof: Since α is an automorphism of M and since L is a subfield of M, we get that $L' = \alpha(L)$ is again a subfield of M. We need to show that $L' = L$.

We first note that $[L' : K] = [L : K]$. Indeed, considering M as a vector space over K and noticing that α is a K-linear mapping of nullity zero, the subspaces L and $L' = \alpha(L)$ must have the same dimension over K, which is exactly the statement $[L : K] = [L' : K]$.

By Definition 3.3.1, L is the smallest subfield of M containing K and R, where R is the set of roots of f in M (same as in L, since f splits over L). Clearly, $\alpha(K) = K$ (in fact, $\alpha(a) = a$ for all $a \in K$). Also, $\alpha(R) = R$ by Proposition 4.2.4. Thus, $K \cup R \subseteq \alpha(L) = L'$. By the minimality of L, we have $L \subseteq L'$.

Since $[L' : K] = [L : K]$, the Tower Law implies $[L' : L] = 1$, that is, $L' = L$. □

We next show that a splitting extension has a significant number of automorphisms.

Proposition 4.3.2 *Let K be a field and L be the splitting field for $f \in K[x]$ over K. Suppose that M and M' are two subfields of L, both containing K. Suppose further that $\theta : M \to M'$ is an isomorphism such that $\theta|_K = id$. Then θ extends to an automorphism of L.*

Proof: Since L is the splitting field for f over K, we also have that L is the splitting field for f over M (and similarly, over M'). Notice that since $\theta|_K = id$, we have $\bar{\theta}(f) = f$, where $\bar{\theta}$ is the polynomial rewriting associated with θ. Thus, by Theorem 3.3.4 there is an isomorphism ϕ from L (the splitting field for f over M) to L (the splitting field for $f = \bar{\theta}(f)$ over M') extending θ. □

Note that this automorphism ϕ is a K-automorphism, that is, an element of $\mathrm{Gal}(L/K)$. Indeed, $\phi|_K = \theta|_K = id$.

Recall that a group G acting on a set R is *transitive* if for all $u, v \in R$ there exists $\alpha \in G$ such that $\alpha(u) = v$.

Corollary 4.3.3 *Suppose K is a field and L is the splitting field for $f \in K[x]$ over K. Suppose $g \in K[x]$ is irreducible and let R be the set of roots of g in L. Then* $\mathrm{Gal}(L/K)$ *is transitive on R.*

Proof: By Proposition 4.2.4, $G = \mathrm{Gal}(L/K)$ acts on R. Suppose $u, v \in R$. Then $\frac{1}{a}g$, where a is the leading coefficient of g, is the minimal polynomial of both u and v. By Corollary 3.2.5, there is an isomorphism θ from $M = K(u)$ to $M' = K(v)$ such that $\theta(u) = v$ and $\theta|_K = id$. Applying Proposition 4.3.2 to this θ, we obtain an element of $\mathrm{Gal}(L/K)$ taking u to v. □

Corollary 4.3.4 *Let K be a field, $f \in K[x]$ and let L be the splitting field for f over K. Write f as $ag_1^{s_1}g_2^{s_2}\cdots g_k^{s_k}$, where $a \in K$ and all $g_i \in K[x]$ are monic irreducible and pairwise different. (Since all g_i are monic, a is the leading coefficient of f.) Let R be the set of roots of f in L, and R_i be the set of roots of g_i, $i = 1, \ldots, k$. Then*

1. *$\{R_i \mid 1 \leq i \leq k\}$ is a partition of R; and*

2. *the orbits of* $\mathrm{Gal}(L/K)$ *on R are precisely the sets $R_1, \ldots, R_k$.*

Proof: Clearly, R is the union of all R_i. If $u \in R_i \cap R_j$, where $i \neq j$, then u is a root of both g_i and g_j. Since g_i and g_j are irreducible and monic, they must be both the minimal polynomial of u, a contradiction. This proves (1).

Now Corollary 4.3.3 applied to $g = g_i$ shows that $\mathrm{Gal}(L/K)$ is transitive on each R_i, yielding (2). □

Example 4.3.5 1. Let L be the splitting field over $\mathbb{Q}$ of $f = x^4 - x^2 - 2 = (x^2+1)(x^2-2)$. Then $G = \mathrm{Gal}(L/\mathbb{Q})$ acts faithfully on the set of roots of f, which is $R = \{i, -i, \sqrt{2}, -\sqrt{2}\}$. By Corollary 4.3.4, G has two orbits on R, namely, $R_1 = \{i, -i\}$ and $R_2 = \{\sqrt{2}, -\sqrt{2}\}$. Thus, the order of G is two or four. Observe that L is the splitting field for $x^2 - 2$ over the Gaussian numbers $\mathbb{Q}(i)$. Since $\sqrt{2} \notin \mathbb{Q}(i)$, $x^2 - 2$ remains irreducible over $\mathbb{Q}(i)$. This means that $\mathrm{Gal}(L/\mathbb{Q}(i))$ is transitive on the set $\{\sqrt{2}, -\sqrt{2}\}$. hence there is an automorphism of L that fixes

$\pm i$ and interchanges $\sqrt{2}$ with $-\sqrt{2}$. Similarly, one can show that there exists an automorphism of L, which fixes $\pm\sqrt{2}$ and which interchanges i with $-i$. We conclude that G has order four, namely, $G \cong S_2 \times S_2$.

2. We can now finish Example 4.2.10 (3). We already know that $G = \mathrm{Gal}(L/\mathbb{Q})$ contains an element of order two, namely, the complex conjugation. Corollary 4.3.4 implies that G is transitive on $\{\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2\}$. Hence the order of G is also divisible by three. Therefore, $|G|$ is at least six, implying that $G \cong \mathrm{Sym}(R) \cong S_3$.

We now start working towards the formal definition of normal extensions.

Proposition 4.3.6 *Let K be a field, $f \in K[x]$, and L be the splitting field for f over K. If $g \in K[x]$ is irreducible and has one root in L, then g splits in L.*

Proof: Let M be the splitting field for g over L. Since M is generated by L and the roots of g and since L is generated by K and the roots of f, we conclude that M is the splitting field for fg over K. (Indeed, the roots of fg are the roots of f plus the roots of g.)

By assumption, g has a root $u \in L$. Let v be any other root of g in M. By Corollary 4.3.3 (applied to the entire M), $\mathrm{Gal}(M/K)$ is transitive on the set of roots of g and so there exists $\alpha \in \mathrm{Gal}(M/K)$, such that $\alpha(u) = v$. According to Proposition 4.3.1, $\alpha(L) = L$, since L is the splitting field for f. This means that $v \in L$, since $u \in L$. Thus, all roots of g are in L. Hence $M = L$ and g splits in L. □

Definition 4.3.7 *An extension $K \subseteq L$ is* normal *if whenever $g \in K[x]$ is irreducible and has at least one root in L, then g splits completely in L.*

So Proposition 4.3.6 states simply that if L is the splitting field over K for some $f \in K[x]$, then $K \subseteq L$ is a normal extension.

Example 4.3.8 1. The extensions $\mathbb{Q} \subseteq \mathbb{Q}(i)$ and $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ are both normal. In fact all extensions of degree two are normal. Indeed, suppose $[L : K] = 2$. Let $u \in L \backslash K$. Then $L = K(u)$ and, in particular, the minimal polynomial of u over K has degree two. Say, $f = x^2 + ax + b$ is the minimal polynomial of u. Notice now that the second root of f is $u' = -a - u \in L$. Hence $L = K(u) = K(u, u')$ is the splitting field for f over K, implying the normality via Proposition 4.3.6.

2. Now consider the degree three extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$. The irreducible polynomial $x^3 - 2$ has a root in $\mathbb{Q}(\sqrt[3]{2})$, but since the other two roots are non-real complex numbers, they cannot be contained in $\mathbb{Q}(\sqrt[3]{2})$. Hence $x^3 - 2$ does not split in $\mathbb{Q}(\sqrt[3]{2})$ and this extension is not normal.

Theorem 4.3.9 *The following are equivalent for a finite extension $K \subseteq L$:*

1. *the extension is normal; and*

2. *L is the splitting field for some polynomial over K.*

Proof: In view of Proposition 4.3.6 it suffices to show that (1) implies (2).

Suppose that $K \subseteq L$ is a finite normal extension. Let $\{u_1, \ldots, u_n\}$ be a basis for L as a vector space over K. For each i, let g_i be the minimal polynomial of u_i over K, and let $f = g_1 \cdots g_n$. Each g_i is irreducible with a root (namely, u_i) in L, so since $K \subseteq L$ is a normal extension, g_i splits in L, that is, it is a product of linear factors in $L[x]$. Hence f is also a product of linear factors in $L[x]$, and so f splits in L. It remains to show that L is generated by the roots of f. However, this is clear, since the roots include $u_1, \ldots, u_n$, and $K(u_1, \ldots, u_n)$ is already all of L. So L is the splitting field for f. □

We conclude this section and the chapter with the following useful observation.

Corollary 4.3.10 *If $K \subseteq L$ is a normal extension and $K \subseteq M \subseteq L$ then $M \subseteq L$ is also normal.*

Proof: By Theorem 4.3.9, L is the splitting field over K for some polynomial $f \in K[x]$. Clearly, L is also the splitting field for the same f over M. □

Chapter 5

Galois correspondence

5.1 Separable extensions

Definition 5.1.1 *Suppose K is a field and $f \in K[x]$ is an irreducible polynomial. We say that f is* separable *if f has no multiple roots. That is, if L is the splitting field for f over K then f has exactly* $\deg(f)$ *distinct roots in L.*

Definition 5.1.2 *For $f = a_nx^n + \cdots + a_0 \in K[x]$ its* derivative *Df is defined by:*

$$Df = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2x + a_1.$$

Here the product of an integer m and a field element a is defined as follows:

$$na = \begin{cases} 0, & \text{if } m = 0; \\ \underbrace{a + \cdots + a}_{n}, & \text{if } n > 0; \\ \underbrace{-a - \cdots - a}_{|n|}, & \text{if } n < 0. \end{cases}$$

(Cf. Section 4.1, where $\rho(n)$ is simply $n1_K$.)

This operation of differentiation has the familiar algebraic properties that the usual calculus differentiation has.

Proposition 5.1.3 *A polynomial $f \in K[x]$ has a multiple root if and only if f and Df have a common divisor, that is, the greatest common divisor (f, Df) is not one.* □

Here is an example of an inseparable irreducible polynomial.

Example 5.1.4

1. Let $K = F(t)$, the field of rational functions in one variable over a field F of positive characteristic p. Consider $f = x^p - t \in K[x]$. Notice that this is a polynomial with just two nonzero coefficients: $a_p = 1_K$ and $a_0 = t \in K = F(t)$. It can be shown (using the so-called Eisenstein criterion, which we don't cover in this course) that f is irreducible. On the other hand, $Df = px^{p-1} = 0$, since $p1_K = \rho(p) = 0$, because K has characteristic p. Clearly, $(f, Df) = (f, 0) = f$ is not equal to one, and so f has multiple roots by Proposition 5.1.3.

2. We again consider $K = F(x)$, where F has positive characteristic p, and the same polynomial $f = x^p - t$. This time we outline a direct proof (without Proposition 5.1.3) that f has multiple roots. Namely, let L be the splitting field of f over K. Then L has the same characteristic p, since L contains K. Let $u \in L$ be a root of f. Then $0 = f(u) = u^p - t$, that is, $u^p = t$. Now we compute $(x - u)^p$ in $L[x]$. By the binomial law, $(x-u)^p = x^p + \binom{p}{1}ux^{p-1} + \cdots + \binom{p}{p-1}u^{p-1}x + u^p = x^p + u^p = x^p - t = f$. (We use here that the binomial coefficient $\binom{p}{k}$, $1 \leq k \leq p-1$, is a multiple of p and hence $\binom{p}{k}u^k = \binom{p}{k}1_K u = \rho(\binom{p}{k})u = 0u = 0$ in L, since L has characteristic p.)

   Thus, $f = (x - u)^p$ in $L[x]$. This means that u is the only root of f in L and so indeed f has multiple roots.

Proposition 5.1.5 *Let K be a field of characteristic zero and $f \in K[x]$ be an irreducible polynomial. Then f has no repeated roots.*

Proof: Since f is irreducible, Df is a nonzero polynomial of degree $n-1$, where $n = \deg(f)$. Indeed, if the leading coefficient of f is $a = a_n \neq 0$ then the leading coefficient of Df is $(n-1)a$, since $(n-1)a = (n-1)1_K a = \rho(n)a \neq 0$, because $a \neq 0$ and also $\rho(n) \neq 0$, since K has characteristic zero.

Thus, Df is nonzero, of degree $n-1$. Suppose f has multiple roots. Then by Proposition 5.1.3, the greatest common divisor (f, Df) is not one, that is, it is a polynomial of positive degree. Let $g = (f, Df)$. Then g divides f, that is, there exists $h \in K[x]$ such that $f = gh$. Since f is irreducible, either g or h is a constant polynomial. In fact, it must be h, because g is known to have positive degree. Thus, h is a constant and hence $\deg(g) = \deg(f) = n$. However, this means that g cannot divide Df, since Df has degree $n-1$; a contradiction. □

Note that the general analog of Proposition 5.1.5 for fields of positive characteristic is not true, as Example 5.1.4 shows. However, the conclusion of this proposition remains true for *some* fields of positive characteristic. For example, it is true for finite fields.

Definition 5.1.6 *A finite field extension $K \subseteq L$ is called* separable *if the minimal polynomial $p = \min_{u,K}$ is separable for each $u \in L$.*

Notice that the minimal polynomial p is always irreducible in $K[x]$ (cf. Proposition 2.3.5) and Definition 5.1.1 can be applied to it.

The following is an immediate consequence of Proposition 5.1.5.

Corollary 5.1.7 *Every finite extension $K \subseteq L$, where $\operatorname{char}(K) = 0$, is separable.* □

Suppose in a separable extension we substitute either K or L with an intermediate field M. Will the resulting extension be again separable? Yes, it will.

Proposition 5.1.8 *Suppose $K \subseteq L$ is a separable extension and suppose $K \subseteq M \subseteq L$. Then both extensions $K \subseteq M$ and $M \subseteq L$ are separable.*

Proof: That $K \subseteq M$ is separable follows directly from the definition, since every element of M is also an element of L.

Let now $u \in L$ and let p and r be the minimal polynomials of u over K and M respectively. Then p has no multiple roots, since $K \subseteq L$ is a separable extension. On the other hand, r divides p in $M[x]$ by Proposition 2.3.10. If in some extension of M r has a multiple root then in the same extension p has the same multiple root; a contradiction. Thus, $r = \min_{u,M}$ has no multiple roots for all $u \in L$. □

5.2 Galois extensions, fixed subfields

Definition 5.2.1 *A finite field extension $K \subseteq L$ is a* Galois extension *if it is normal and separable.*

Notice that for fields of zero characteristic (in particular, for all extensions of $\mathbb{Q}$—which is the main case as far as this course is concerned) all finite extensions are automatically separable by Corollary 5.1.7. So normality is all we need to satisfy in this case.

The property of being Galois is inherited by intermediate extensions, in the following sense.

Proposition 5.2.2 *Suppose $K \subseteq L$ is a Galois extension and suppose M is an intermediate field, that is, $K \subseteq M \subseteq L$. Then $M \subseteq L$ is also a Galois extension.*

Proof: First of all, $M \subseteq L$ is a finite extension by the Tower Law. Also, $M \subseteq L$ is separable by Proposition 5.1.8. Finally, Corollary 4.3.10 yields that $M \subseteq L$ is normal. □

Note that the extension $K \subseteq M$, though being finite and separable, does not need to be normal and hence it does not need to be Galois.

We will now see what this property (being Galois) means for the Galois group of the extension.

Theorem 5.2.3 *Suppose $K \subseteq L$ is a Galois extension. Then* $|\mathrm{Gal}(L/K)| = [L : K]$.

Proof: We proceed by induction on $n = [L : K]$. If $n = 1$, then $L = K$, and so $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/L) = 1$. Now suppose that $n > 1$. It follows from normality and Theorem 4.3.9 that L is the splitting field for some $f \in K[x]$. Since $L > K$ and since L is generated by the roots of f, there exists some root u with $u \notin K$. Let $p \in K[x]$ be the minimal polynomial of u over K. By Corollary 4.3.3 (or Corollary 4.3.4), the set of roots of p, say R, coincides with the orbit of u under the action of $G = \mathrm{Gal}(L/K)$. Notice that p divides f, since $f(u) = 0$. Thus, the roots of p are also roots of f. Since f splits in L (that is, it has no new roots in any extension of L), so also does p. By separability, $p = \min_{u,K}$ has no multiple roots, which means that p has exactly $\deg(f)$ distinct roots; that is, $|R| = \deg(p)$.

Since G acts transitively on R, we have the equality $|G| = |R||G_u|$ by the Orbit–Stabilizer theorem. By the above, $|R| = \deg(p)$, which, in turn, is equal to $[K(u) : K]$ by Theorem 3.1.3. Also, $G_u = \mathrm{Gal}(L/K(u))$ by Proposition 4.2.6. Notice that $M = K(u) > K$ and so $[L : M] < [L : K] = n$ by the Tower Law. Notice also that the extension $M \subseteq L$ is Galois by Proposition 5.2.2. So it satisfies the assumptions of our theorem. By induction, since $[L : M] < n$, we have that $|\mathrm{Gal}(L/M)| = [L : M]$.

Putting everything together, we obtain the sequence of equalities: $|G| = |R||G_u| = \deg(p)\,|G_u| = [K(u) : K]|G_u| = [K(u) : K]|\mathrm{Gal}(L/K(u))| = [M : K]|\mathrm{Gal}(L/M)| = [M : K][L : M]$. By the Tower Law, the latter is $[L : K]$. □

Definition 5.2.4 *Let L be a field and H a subgroup of* $\mathrm{Aut}(L)$. *The* fixed subfield *of H in L is* $\mathrm{Fix}(H) = \{a \in L \,|\, \alpha(a) = a \text{ for all } \alpha \in H\}$.

We leave it as an exercise to check that $\mathrm{Fix}(H)$ is indeed a subfield. The following proposition summarizes the basic properties of fixed subfields.

Proposition 5.2.5 *Suppose L is a field and* $G = \mathrm{Aut}(L)$.

1. *If $H = 1$ is the trivial (identity) subgroup of G then* $\mathrm{Fix}(H) = L$.

2. *If $J \leq H \leq G$ then* $\mathrm{Fix}(H) \subseteq \mathrm{Fix}(J)$

3. *If $H \leq G$ and $K =$* $\mathrm{Fix}(H)$ *then $H \leq$* $\mathrm{Gal}(L/K)$.

4. *If K is a subfield of L and $H =$* $\mathrm{Gal}(L/K)$ *then $K \subseteq$* $\mathrm{Fix}(H)$. □

How does one compute the fixed subfield for a given subgroup H? For $\alpha \in \mathrm{Aut}(L)$ set $\mathrm{Fix}(\alpha) = \{a \in L \,|\, \alpha(a) = a\}$. Thus, Definition 5.2.4 just tells us that

$$\mathrm{Fix}(H) = \cap_{\alpha \in H} \mathrm{Fix}(\alpha).$$

As the following statement (also left as an exercise) shows, we can leave in this intersection only a small set of α's that generates H (instead of all elements of H).

Proposition 5.2.6 *Suppose A is a subset of* $\mathrm{Aut}(L)$ *and $H = \langle A \rangle$. Then* $\mathrm{Fix}(H) = \cap_{\alpha \in A} \mathrm{Fix}(\alpha)$. □

This allows us to ignore most of the elements of H. Next, suppose that A and $H = \langle A \rangle$ lie in $G = \mathrm{Gal}(L/K)$ for a finite extension $K \subseteq L$. Then every $\alpha \in A$ is a K-automorphism of L, that is, α turns into a linear transformation $T_\alpha : L \to L$, where L is viewed as a vector space over K. (This transformation is, really, α itself, that is, $T_\alpha(v) = \alpha(v)$ for $v \in L$.) From the linear algebra point of view, $\mathrm{Fix}(\alpha)$ is a subspace of L, namely, $\mathrm{Fix}(\alpha)$ is the *eigenspace* of T_α corresponding to the *eigenvalue* 1 (since $T_\alpha(v) = \alpha(v) = v = 1_K v$, for $v \in \mathrm{Fix}(\alpha)$.) Thus, finding the fixed subfield is essentially a linear algebra problem, which can be done efficiently on a computer (but not by hand, unless $[L : K]$ is small).

The following important result will be needed in the next section. We skip the proof because it would take us out of the boundaries set for the course.

Proposition 5.2.7 *Suppose L is a field and G is a finite subgroup of* $\mathrm{Aut}(L)$. *Let $K = \mathrm{Fix}(G)$. Then $[L : K] \leq |G|$.* □

This result is really all we will need in the final section. However, a lot more can be proved under the same assumptions, as the following final result of the section shows.

Theorem 5.2.8 *Suppose L is a field and G is a finite subgroup of* $\mathrm{Aut}(L)$. *Set $K = \mathrm{Fix}(G)$. Then $K \subseteq L$ is a Galois extension and $G = \mathrm{Gal}(L/K)$. In particular, $|G| = [L : K]$.*

Proof: Let $u \in L$ and let $T = \{\alpha(u) \mid \alpha \in G\}$ be the orbit of u under the action of G. Clearly, T is a finite set. Define $p = \prod_{v \in T}(x - v) \in L[x]$. For $\alpha \in G$, let $\bar{\alpha}$ be the corresponding polynomial rewriting on $L[x]$. Then $\bar{\alpha}(p) = \prod_{v \in T} \bar{\alpha}(x - v) = \prod_{v \in T}(x - \alpha(v)) = p$. The first equality here is due to the fact that $\bar{\alpha}$ is a homomorphism, and the last equality is due to the fact that α permutes the orbit T, so we have the same linear factors, as in p, but possibly in a different order.

If $p = a_k x^k + \cdots + a_0$ then $\bar{\alpha}(p) = \alpha(a_k)x^k + \cdots + \alpha(a_0)$. Thus, the equality $\bar{\alpha}(p) = p$ means that $\alpha(a_i) = a_i$ for all coefficients a_i of p. That is, every a_i is contained in $\mathrm{Fix}(\alpha)$ for all $\alpha \in G$. Therefore, every a_i is contained in $K = \mathrm{Fix}(G)$. We have established that $p \in K[x]$.

Notice that p is monic since it the product of monic linear factors, and also notice that $p(u) = 0$, since $u \in T$. By Proposition 5.2.5 (3), $G \leq \mathrm{Gal}(L/K)$, so by Corollary 4.2.5, T is a subset of the set of roots of the minimal polynomial $\min_{u,K}$. This means that $\deg(\min_{u,K}) \geq |T| = \deg(p)$. On the other hand, $\deg(\min_{u,K}) \leq \deg(p)$, since $p(u) = 0$ and hence $\min_{u,K}$ divides p. We conclude that $\deg(p) = \deg(\min_{u,K})$ and hence $p = \min_{u,K}$.

On the one hand, this means that the extension $K \subseteq L$ is separable, since $p = \min_{u,K}$ has exactly $\deg(p) = |T|$ distinct roots, for all $u \in L$. On the other hand, we also get the normality. Indeed, if $g \in K[x]$ is irreducible and g has a root in L, say, u. Then $\frac{1}{a}g = \min_{u,K} = p$, where a is the leading coefficient of g. By the above, p splits in L, and hence so does g, implying by Definition 4.3.7 that $K \subseteq L$ is normal. Thus, $K \subseteq L$ is a Galois extension (finiteness of the extension follows from Proposition 5.2.7).

Since $G \leq \mathrm{Gal}(L/K)$, Theorem 5.2.3 implies that $|G| \leq |\mathrm{Gal}(L/K)| = [L : K]$. Since $|G| \geq [L : K]$ by Proposition 5.2.7, we obtain $|G| = [L : K]$, which yields $G = \mathrm{Gal}(L/K)$. □

5.3 Fundamental Theorem of Galois Theory

Let $K \subseteq L$ be a Galois extension. The Fundamental Theorem of Galois Theory (FTGT) relates the structure of the extension $K \subseteq L$ to the structure of the group $\mathrm{Gal}(L/K)$. This is the main theorem of this course, and its statement and subsequent proof will be split up and summarized at the end.

Let $\mathcal{F} = \{M \mid K \leq M \leq L\}$ be the set of all intermediate subfields of the extension. Let $\mathcal{G}$ be the set of all subgroups of $G = \mathrm{Gal}(L/K)$. Define a map $\Phi : \mathcal{F} \to \mathcal{G}$ by

$$\Phi(M) = \mathrm{Gal}(L/M),$$

and a map $\Psi : \mathcal{G} \to \mathcal{F}$ by

$$\Psi(H) = \mathrm{Fix}(H).$$

The following result contains the first two parts of the FTGT.

Theorem 5.3.1 *1. The mappings Φ and Ψ are bijective; furthermore, $\Phi^{-1} = \Psi$; i.e., for all $M \in \mathcal{F}$ we have $M = \mathrm{Fix}(\mathrm{Gal}(L/M))$, and for all $H \in \mathcal{G}$ we have $H = \mathrm{Gal}(L/\mathrm{Fix}(H))$.*

2. Φ and Ψ are both order-reversing; that is, for $M_1, M_2 \in \mathcal{F}$, $M_1 \subseteq M_2$, we have $\Phi(M_2) \leq \Phi(M_1)$, and for $H_1, H_2 \in \mathcal{G}$, $H_1 \leq H_2$, we have $\Psi(H_2) \subseteq \Psi(H_1)$.

Proof: We first show that $\mathrm{Gal}(L/\mathrm{Fix}(H)) = H$ for all $H \in \mathcal{G}$. Let $M = \mathrm{Fix}(H)$. Thus, we need to see that $H = \mathrm{Gal}(L/M)$. By Proposition 5.2.5 (3), $H \leq \mathrm{Gal}(L/M)$. Notice that $M \subseteq L$ is a Galois extension by Proposition 5.2.2. Hence, by Theorem 5.2.3, $|\mathrm{Gal}(L/M)| = [L : M]$. Therefore, $|H| \leq |\mathrm{Gal}(L/M)| = [L : M] \leq |H|$ (the second inequality is due to Proposition 5.2.7). Clearly, this means that both inequalities here are in fact equalities. In particular, $|H| = |\mathrm{Gal}(L/M)|$, yielding $H = \mathrm{Gal}(L/M)$.

Next, for an arbitrary $M \in \mathcal{F}$, let $H = \mathrm{Gal}(L/M)$ and $M' = \mathrm{Fix}(H)$. We need to see that $\mathrm{Fix}(\mathrm{Gal}(L/M)) = M$, that is, $M' = M$. By Proposition 5.2.5 (4), $M \subseteq M'$. Furthermore, by the above, $H = \mathrm{Gal}(L/M')$. Since both extensions $M \subseteq L$ and $M' \subseteq L$ are Galois by Proposition 5.2.2, Theorem 5.2.3 now gives $[L : M] = |H| = [L : M']$. Hence $[L : M] = [L : M']$. By the Tower Law we now get $[M' : M] = 1$, yielding $M' = M$.

Part (2) of our theorem is a combination of Proposition 4.2.2 (3) and Proposition 5.2.5 (2). □

Traditionally, the third part of the FTGT is the claim that $|\mathrm{Gal}(L/M)| = [L : M]$ for all $M \in \mathcal{F}$. Since this has already been proven in Theorem 5.2.3, we insert here a statement that gives slightly more.

Proposition 5.3.2 *If $M, M' \in \mathcal{F}$ and $M \subseteq M'$ then $[M' : M] = [\Phi(M) : \Phi(M')]$. Equivalently, if $H, H' \in \mathcal{G}$ and $H \geq H'$ then $[H : H'] = [\Psi(H') : \Psi(H)]$.*

Proof: We will prove the first statement. We have $[\Phi(M) : \Phi(M') = [\mathrm{Gal}(L/M) : \mathrm{Gal}(L/M')] = \frac{|\mathrm{Gal}(L/M)|}{|\mathrm{Gal}(L/M')|} = \frac{[L:M]}{[L:M']} = [M' : M]$. The last equality is due to the Tower Law. □

Corollary 5.3.3 *If $M \in \mathcal{F}$ then $[M : K] = [G : \Phi(M)] = [G : \mathrm{Gal}(L/M)]$, where $G = \mathrm{Gal}(L/K)$.*

Proof: Apply Proposition 5.3.2 to the subfields K and M. □

We discuss two examples.

Example 5.3.4 1. Consider $L = \mathbb{Q}(\sqrt{2}, i)$. We already know (cf. Example 4.3.5 (1)) that L is the splitting field for $f = (x^2 - 2)(x^2 + 1) = x^4 - x^2 - 2$, hence $\mathbb{Q} \subseteq L$ is Galois. We also determined that $[L : \mathbb{Q}] = |\mathrm{Gal}(L/\mathbb{Q})| = 4$. More precisely, $G = \mathrm{Gal}(L/\mathbb{Q})$ is generated by two elements: α, induced by the complex conjugation, fixes $\pm\sqrt{2}$ and interchanges $\pm i$; similarly, β fixes $\pm i$ and interchanges $\pm\sqrt{2}$. It follows that $G = \langle\alpha\rangle \times \langle\beta\rangle \cong V_4$, the Klein four group.

The subgroups of G are the trivial subgroup 1, the entire G, and three intermediate subgroups: $\langle\alpha\rangle$, $\langle\beta\rangle$, and $\langle\alpha\beta\rangle$. Let us determine $\Psi(H)$ for all these subgroups H. Clearly, $\Psi(1) = L$ and $\Psi(G) = \mathbb{Q}$. Also, α fixes all of $\mathbb{Q}(\sqrt{2})$, hence the latter field is $\Psi(\langle\alpha\rangle)$. Similarly, $\mathbb{Q}(i) = \Psi(\langle\beta\rangle)$. It remains to determine $\Psi(\langle\alpha\beta\rangle)$. Notice that $\sqrt{2}i \in L$ and $\alpha\beta(\sqrt{2}i) = \alpha(-\sqrt{2}i) = -\sqrt{2}(-i) = \sqrt{2}i$. Clearly, $\sqrt{2}i \notin \mathbb{Q}$ and so $\mathbb{Q}(\sqrt{2}i) = \Psi(\langle\alpha\beta\rangle)$.

2. Here is a slightly more complicated example. Let L be the splitting field of $x^3 - 2$. In Example 4.3.5 (2) we determined that $\mathrm{Gal}(L/Q)$ induces on the set $R = \{\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2\}$, where $\zeta = e^{\frac{2\pi i}{3}}$, the full group $\mathrm{Sym}(R) \cong S_3$.

The group $\mathrm{Sym}(R)$ can be generated by two elements: α fixes $\sqrt[3]{2}$ and interchanges the other two elements of R (α is induced by the complex conjugation); β induces a 3-cycle on R, namely, $\beta(\sqrt[3]{2}) = \sqrt[3]{2}\zeta$, $\beta(\sqrt[3]{2}\zeta) = \sqrt[3]{2}\zeta^2$, and $\beta(\sqrt[3]{2}\zeta^2) = \sqrt[3]{2}$. Then the subgroups of

$G = \mathrm{Sym}(R)$ are as follows: 1, G, $\langle\beta\rangle$ (of order three), $\langle\alpha\rangle$, $\langle\alpha\beta\rangle$, and $\langle\alpha\beta^2\rangle$ (the last three subgroups are of order two).

Let us determine the subfields of L. Clearly, $\Psi(1) = L$ and $\Psi(G) = \mathbb{Q}$. Since α fixes $\sqrt[3]{2}$, we have $\mathbb{Q}(\sqrt[3]{2}) = \Psi(\langle\alpha\rangle)$ (cf. Proposition 4.2.6). Similarly, by direct computation, $\alpha\beta$ fixes $\sqrt[3]{2}\zeta$ and $\alpha\beta^2$ fixes $\sqrt[3]{2}\zeta^2$. Therefore, $\mathbb{Q}(\sqrt[3]{2}\zeta) = \Psi(\langle\alpha\beta\rangle)$ and $\mathbb{Q}(\sqrt[3]{2}\zeta^2) = \Psi(\langle\alpha\beta^2\rangle)$.

It remains to determine $\Psi(\langle\beta\rangle)$. However, β does not fix any roots from R. What should we do? Notice that $\zeta = \frac{\sqrt[3]{2}\zeta}{\sqrt[3]{2}} \in L$. Furthermore, the minimal polynomial of ζ is $\frac{x^3-1}{x-1} = x^2+x+1$. Therefore, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$ and so $[L : \mathbb{Q}(\zeta)] = \frac{[L:\mathbb{Q}]}{[\mathbb{Q}(\zeta):\mathbb{Q}]} = \frac{6}{2} = 3$. Thus, the subfield $\mathbb{Q}(\zeta)$ must correspond to a subgroup $H \leq G$ of order three. Since $\langle\beta\rangle$ is the only such subgroup, we conclude that $\Psi(\langle\beta\rangle) = \mathbb{Q}(\zeta)$.

If $\alpha \in G = \mathrm{Gal}(L/K)$ and $M \in \mathcal{F}$ then $\alpha(M)$ is also an intermediate subfield, *i.e.,* it belongs to $\mathcal{F}$. What is the relation between the subgroups $\Phi(M)$ and $\Phi(\alpha(M))$ of G?

Proposition 5.3.5 *Let* $\alpha \in G = \mathrm{Gal}(L/K)$*, and* $M \in \mathcal{F}$*. Then*

$$\Phi(\alpha(M)) = \alpha\Phi(M)\alpha^{-1}.$$

So $\mathrm{Gal}(L/M) = \Phi(M) \trianglelefteq G$ *if and only if* $\alpha(M) = M$ *for all* $\alpha \in G$*.*

Proof: For $\beta \in G$ set $\beta' = \alpha^{-1}\beta\alpha$.

Suppose first that $\beta \in \Phi(\alpha(M)) = \mathrm{Gal}(L/\alpha(M))$. This means that β fixes every element $a \in \alpha(M)$. Suppose $b \in M$. Then $\beta'(b) = \alpha^{-1}\beta\alpha(b) = \alpha^{-1}\beta(\alpha(b)) = \alpha^{-1}(\alpha(b)) = b$. Here we used that $\alpha(b) \in \alpha(M)$ and hence $\beta(\alpha(b)) = \alpha(b)$. Since $\beta'(b) = b$ for all $b \in M$, we have that $\beta' \in \mathrm{Gal}(L/M) = \Phi(M)$, and hence $\beta = \alpha\beta'\alpha^{-1} \in \alpha\Phi(M)\alpha^{-1}$, proving that $\Phi(\alpha(M)) \leq \alpha\Phi(M)\alpha^{-1}$.

For the reverse inclusion, suppose $\beta \in \alpha\Phi(M)\alpha^{-1}$, that is, $\beta' \in \Phi(M) = \mathrm{Gal}(L/M)$. For $a \in \alpha(M)$ let $b \in M$ be such that $a = \alpha(b)$ (in fact, $b = \alpha^{-1}(a)$). Then $\beta(a) = \alpha\beta'\alpha^{-1}(a) = \alpha\beta'(b) = \alpha(b) = a$, where $\beta'(b) = b$, since $b \in M$. Thus, $\beta(a) = a$ for all $a \in \alpha(M)$, that is, $\beta \in \mathrm{Gal}(L/\alpha(M)) = \Phi(\alpha(M))$.

So $\Phi(\alpha(M)) = \alpha\Phi(M)\alpha^{-1}$. If $\Phi(M)$ is normal in G, then $\Phi(\alpha(M)) = \Phi(M)$ and vice versa. Since Φ is a bijection, $\alpha(M) = M$ for all $\alpha \in G$. □

This proposition is needed to prove part four of the FTGT. Recall that the extension $M \subseteq L$ is Galois for all $M \in \mathcal{F}$. However, this is not in general true for the extension $K \subseteq M$.

Theorem 5.3.6 *For $M \in \mathcal{F}$, the extension $K \subseteq M$ is Galois if and only if $\mathrm{Gal}(L/M) = \Phi(M) \trianglelefteq G = \mathrm{Gal}(L/K)$.*

Proof: Suppose the extension $K \subseteq M$ is Galois. Then $K \subseteq M$ is a normal extension and hence M is the splitting field of some polynomial $f \in K[x]$. According to Proposition 4.3.1 this means that $\alpha(M) = M$ for all $\alpha \in G$. By Proposition 5.3.5, it now follows that $\mathrm{Gal}(L/M) = \Phi(M) \trianglelefteq G$.

Now suppose that $\Phi(M) = \mathrm{Gal}(L/M)$ is normal in $G = \mathrm{Gal}(L/K)$, which means, by Proposition 5.3.5, that $\alpha(M) = M$ for all $\alpha \in G$. Clearly, the extension $K \subseteq M$ is finite and separable, since $K \subseteq L$ is finite and separable. So we just need to see that $K \subseteq M$ is a normal extension. Suppose $g \in K[x]$ is an irreducible polynomial, having a root, say u, in M. We need to show that g splits in M. Since $K \subseteq L$ is normal, g splits in L. Let R be the set of roots of g in L. By Corollary 4.3.3, G acts transitively on R. If $v \in R$ then, by the transitivity, there exists $\alpha \in G$, such that $v = \alpha(u)$. Since $u \in M$ and $\alpha(M) = M$, we obtain that $v \in M$. Thus, $R \subseteq M$, which means that g splits already in M. This verifies Definition 4.3.7. Therefore, the extension $K \subseteq M$ is normal, and hence it is Galois. □

Suppose $K \subseteq M$ is Galois for some $M \in \mathcal{F}$. Can we determine the Galois group of this extension? The answer to this is given by part five of the FTGT.

Theorem 5.3.7 *If $M \in \mathcal{F}$ and the extension $K \subseteq M$ is Galois, then $\mathrm{Gal}(M/K) \cong G/\mathrm{Gal}(L/M)$, where $G = \mathrm{Gal}(L/K)$.*

Proof: By Theorem 5.3.6, $\mathrm{Gal}(M/K) \trianglelefteq G$ and so the above factor group makes sense. By Proposition 5.3.5, we also know that $\alpha(M) = M$ for all $\alpha \in G$. Consider the mapping $\pi : \alpha \mapsto \alpha|_M$. This mapping π is a homomorphism from G to $\mathrm{Gal}(M/K)$, since $\alpha|_M \in \mathrm{Gal}(M/K)$ for all $\alpha \in G$. Observe that $\ker \pi = \{\alpha \in G \,|\, \alpha|_M = id\}$. Thus, $\ker \pi = \mathrm{Gal}(L/M)$. By Proposition 4.3.2, every $\beta \in \mathrm{Gal}(M/K)$ extends to some $\alpha \in G$. Hence $\operatorname{im}\pi = \mathrm{Gal}(M/K)$. Now the first isomorphism theorem yields the required isomorphism. $\square$

We remark that the equality $\operatorname{im}\pi = \mathrm{Gal}(M/K)$ could also be established by counting. Namely, $|\operatorname{im}\pi| = \frac{|G|}{|\ker\pi|} = \frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/M)|} = \frac{[L:K]}{[L:M]} = [M : K] = |\mathrm{Gal}(M/K)|$. So we must have $\operatorname{im}\pi = \mathrm{Gal}(M/K)$.

Let us see what all these results give us for the two fields from Example 5.3.4.

Example 5.3.8 1. If $L = \mathbb{Q}(\sqrt{2}, i)$ then the group $G = \mathrm{Gal}(L/\mathbb{Q})$ is abelian, which means that the operation of conjugation (as in Proposition 5.3.5) is trivial. Hence every automorphism of L stabilizes every subfield of L. In particular, the three intermediate subfields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, and $\mathbb{Q}(\sqrt{2}i)$ are Galois extensions of $\mathbb{Q}$. Furthermore, in each of the three cases $\mathrm{Gal}(M/\mathbb{Q}) \cong G/\Phi(M)$ is of order two.

2. Let now $L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ be the splitting field of $x^3 - 2$. In this case $G = \mathrm{Gal}(L/\mathbb{Q}) \cong S_3$ is nonabelian, hence conjugation is a nontrivial operation. The subgroup $\langle\beta\rangle$ has index two in G and hence, by a well-known fact from the group theory, it is normal in G. This means that the corresponding subfield $\mathbb{Q}(\zeta)$ is left invariant by all automorphisms of L, and the extension $\mathbb{Q} \subseteq \mathbb{Q}(\zeta)$ is a Galois extension. We get now that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong G/\langle\beta\rangle$ is of order two. The nontrivial element from $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ can be obtained by restricting α (complex conjugation!) to $\mathbb{Q}(\zeta)$.

   We know that $\beta(\sqrt[3]{2}) = \sqrt[3]{2}\zeta$. Hence $\beta(\mathbb{Q}(\sqrt[3]{2})) = \mathbb{Q}(\sqrt[3]{2}\zeta)$, which corresponds to the fact that $\beta\langle\alpha\rangle\beta^{-1} = \langle\alpha\beta\rangle$ (this can be verified directly in G). Similarly, $\beta(\mathbb{Q}(\sqrt[3]{2}\zeta)) = \mathbb{Q}(\sqrt[3]{2}\zeta^2)$ and $\beta\langle\alpha\beta\rangle\beta^{-1} = \langle\alpha\beta^2\rangle$. Finally, $\beta(\mathbb{Q}(\sqrt[3]{2}\zeta^2)) = \mathbb{Q}(\sqrt[3]{2})$ and $\beta\langle\alpha\beta^2\rangle\beta^{-1} = \langle\alpha\rangle$.

   In particular, none of the subfields $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}\zeta)$, and $\mathbb{Q}(\sqrt[3]{2}\zeta^2)$ is a Galois extension of $\mathbb{Q}$.

We conclude with a summary of the FTGT:

Theorem 5.3.9 (Fundamental Theorem of Galois Theory) *Suppose $K \subseteq L$ is a Galois extension and let $\mathcal{F}$, $\mathcal{G}$, Φ, and Ψ be as before.*

1. *Φ and Ψ are bijective; more precisely, $\Phi^{-1} = \Psi$.*

2. *Φ and Ψ are order-reversing.*

3. *If $M \in \mathcal{F}$, then $[L : M] = |\mathrm{Gal}(L/M)|$.*

4. *If $M \in \mathcal{F}$ then $K \subseteq M$ is Galois if and only if $\mathrm{Gal}(L/M) \trianglelefteq \mathrm{Gal}(L/K)$.*

5. *If $M \in \mathcal{F}$ and $K \subseteq M$ is Galois, then*

$$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M).$$