Notes on Galois Theory

Paul D. Mitchener

October 16, 2007

Contents

1 Introduction

The purpose of these notes is to look at the theory of field extensions and Galois theory, along with some of the more well-known applications. The reader is assumed to be familiar with linear algebra, and to know about groups, rings, fields, and other elementary algebraic objects.

All fields in these notes are commutative. All rings are commutative, and have an identity element.

2 Extensions

Let E be a field, and let F be a subfield of E. Then we call E an *extension* of F, and write $F < E$. Amongst other properties, the field E is a vector space over the field F.

Definition 1 Let $F < E$, and let $\alpha, \beta, \gamma, \ldots$ be elements of E. Then we define $F[\alpha, \beta, \gamma, \ldots]$ to be the subfield of E consisting of all quotients of polynomials in the elements $\alpha, \beta, \gamma, \ldots$ with coefficients in the field F. We call the field $F[\alpha, \beta, \gamma, \ldots]$ the field obtained from F by *adjunction* of the elements $\alpha, \beta, \gamma, \ldots$, or the field *generated* from F by the elements $\alpha, \beta, \gamma, \ldots$.

The field $F[\alpha, \beta, \gamma, \ldots]$ is clearly the smallest extension of F containing the elements $\alpha, \beta, \gamma, \ldots$.

Definition 2 Let $F < E$ be an extension. Then the *degree* of the extension, $\deg(E/F)$, is the dimension of the set E when considered as a vector space over the field F. We call the extension E *finite* if $\deg(E/F) < \infty$.

Example 3 Let F be a field. Then the extension F^n has degree n over F.

Example 4 The extension $\mathbb{C}$ of the field $\mathbb{R}$ has degree 2.

Example 5 The extension $\mathbb{R}$ of the field $\mathbb{Q}$ has infinite degree.

Proposition 6 *Let F be a field. Let B be a finite extension of F, and let E be a finite extension of B. Then*

$$\deg(E/F) = \deg(B/F)\deg(E/B)$$

Proof: Let $\deg(E/B) = m$ and $\deg(B/F) = n$. Let $\{e_1, \ldots, e_m\}$ be a basis of E with respect to B, and $\{b_1, \ldots, b_n\}$ be a basis of B with respect to F. Then it is straightforward to check that the set

$$\{b_i e_j \mid 1 \leq i \leq n,\ 1 \leq j \leq m\}$$

is a basis of E with respect to F. □

The above result, suitably interpreted, also holds for infinite extensions.

Corollary 7 *Let $F < F_1 < \ldots < F_n$ be a sequence of finite extensions. Then*

$$\deg(F_n/F) = \deg(F_n/F_{n-1})\deg(F_{n-1}/F_{n-2})\cdots\deg(F_2/F_1)\deg(F_1/F)$$

□

Exercises

1. Complete the proof of proposition 6
2. Let F be a field. Let B be an extension of F, and let E be an extension of B. Suppose $\deg(B/F) = \infty$ or $\deg(E/B) = \infty$. Prove that $\deg(E/F) = \infty$.
3. Prove that $\deg(\mathbb{R}/\mathbb{Q}) = \infty$.
4. Let E be a field, and let F and F' be subfields such that $\deg(E/F) = \deg(E/F')$. Prove that $F = F'$.

3 Euclidean Rings

This section contains no proofs.

Definition 8 Let R be a ring. We call R an *integral domain* if the product of any two non-zero elements is non-zero.

An integral domain R is termed a *Euclidean domain* if it comes equipped with a function $d\colon R\backslash\{0\} \to \mathbb{Z}$ such that:

- $d(a) \leq d(ab)$ for all $a, b \in R\backslash\{0\}$.
- Let $a, b \in R\backslash\{0\}$. Then there are unique elements $m, r \in R$ such that $a = mb + r$ and $d(r) < d(b)$ or $r = 0$.

Example 9 Any field is an integral domain.

Example 10 The ring of integers, $\mathbb{Z}$, equipped with the function $d(k) = |k|$, is a Euclidean domain.

The formula in the definition of a Euclidean domain is called the *division algorithm.*

Definition 11 Let R be a ring. Then we call an element $a \in R$ a *factor* of $b \in R$ if we can find $c \in R$ such that $b = ac$.

We have already defined and looked at factors in the special case of the polynomial ring.

Definition 12 Let R be a ring. Let $x, y \in R$. Then we call an element $d \in R$ a *greatest common divisor* of x and y if:

- d is a factor of x and y.

- Whenever an element $c \in R$ is a factor of both x and y, the element c is also a factor of d.

Theorem 13 *Let R be a Euclidean domain. Let $x, y \in R$. Then a and b have a greatest common divisor, d. Further, we can find $m, n \in R$ such that*

$$d = ma + nb$$

□

If d is a highest common factor of two elements x and y, and there is an element d' and invertible element u such that $d' = du$, then d' is also a highest common factor.

Example 14 In the field $\mathbb{Z}$, the highest common factor of the numbers 9 and 6 is 3. We can write

$$3 = 9 - 6$$

The number -3 is also a highest common factor of 9 and 6.

Definition 15 Two elements $x, y \in R$ are said to have *no non-trivial common factors* if they have highest common factor 1.

Proposition 16 *Elements $x, y \in R$ have no non-trivial common factors if and only if we can find $m, n \in R$ such that*

$$ma + nb = 1$$

□

Exercises

1. Find an example of a ring that is not an integral domain.
2. Is it possible for a field to be an integral domain?

4 Polynomials

Given a field F, we can form the ring $F[x]$ of all polynomials over the field F. Such a polynomial can be considered a formal expression of the form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

where $a_i \in F$. Addition and multiplication of polynomials are defined in the obvious way.

The elements $a_i \in F$ are called the *coefficients* of the polynomial. We say that the polynomial $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ has *degree* n provided $a_n \neq 0$. We write $\deg p(x)$ to denote the degree of a polynomial $p(x) \in F(x)$. Given non-zero polynomials $q(x), r(x) \in F(x)$, the following formula clearly holds

$$\deg(q(x)r(x)) = \deg q(x) + \deg r(x)$$

The set of all polynomials of degree n, along with the zero polynomial (which it is convenient to say has degree n for *all* n) forms of vector space over F, with dimension $n + 1$. A degree 0 polynomial is simply a *constant*, that is to say an element of the field F.

Definition 17 Let $p(x), q(x) \in F[x]$ be polynomials. We say that $q(x)$ is a *factor* of the polynomial $p(x)$ if there is another polynomial $k(x)$ such that $p(x) = k(x)q(x)$.

We call the polynomial $p(x)$ *irreducible* if it only has factors of degree 0.

We term a degree 0 factor of a polynomial *trivial*. The following result can be proved by induction using the degree formula.

Proposition 18 *Every polynomial is a finite product of irreducible polynomials.* □

Later on, we will see that such factorisations are essentially unique.

Much of our work involving polynomials uses the following.

Proposition 19 *Let F be a field. Then the ring $F[x]$, equipped with the degree function, is a Euclidean domain.* □

Thus, the product of any two non-zero polynomials is not zero, and given polynomials $p(x)$ and $q(x)$, there are polynomials $m(x)$ and $r(x)$ such that

$$p(x) = m(x)q(x) + r(x) \qquad \deg r(x) < \deg q(x) \text{ or } r(x) = 0$$

The proof of the following result is an illustration of the division algorithm.

Proposition 20 *Let $p(x) \in F[x]$ be irreducible, with degree n. Let $q_1(x)$ and $q_2(x)$ be non-zero polynomials of degree less than n. Then $p(x)$ is not a factor of the product $q_1(x)q_2(x)$.*

Proof: Suppose we can find non-zero polynomials $q_1(x)$ and $q_2(x)$ of degree less than n such that $p(x)$ is a factor of the product $q_1(x)q_2(x)$. Then we can choose the polynomial $q_1(x)$ to have the smallest possible degree such that the above fact can still hold.

Since the polynomial $p(x)$ is a factor of the product $q_1(x)q_2(x)$, we can find a polynomial $k(x)$ such that

$$k(x)p(x) = q_1(x)q_2(x)$$

By the division algorithm, we can find polynomials $m(x)$ and $r(x)$ such that

$$p(x) = m(x)q_1(x) + r(x)$$

where $\deg r(x) < \deg q(x)$, and $r(x) \neq 0$ since $p(x)$ is irreducible. Hence

$$r(x)q_2(x) = p(x)q_2(x) - m(x)q_1(x)q_2(x) = p(x)(q_2(x) - m(x)k(x))$$

Therefore the polynomial $p(x)$ is a factor of the product $r(x)q_2(x)$. But $\deg r(x) < \deg q_1(x)$, which contradicts our choice of $q_1(x)$ as being of smallest possible degree such that $p(x)$ is a factor of $q_1(x)q_2(x)$.

Thus no such $q_1(x)$ exists, and we are done. □

The following result comes from applying proposition 16 to the polynomial ring.

Proposition 21 *Let $p(x), q(x) \in F[x]$. Then $p(x)$ and $q(x)$ have no non-trivial common factor if and only if there are polynomials $m(x)$ and $n(x)$ such that*

$$m(x)p(x) + n(x)q(x) = 1$$

□

If E is an extension of a field F, and $p(x) \in F[x]$, then we can also consider $p(x)$ to lie in $E[x]$.

Corollary 22 *Let $p(x), q(x) \in F[x]$. Let E be an extension of F. Then $p(x)$ and $q(x)$ have no non-trivial common factors in $E[x]$ if and only if they have no non-trivial common factors in $F[x]$.* □

Exercises

1. Let $f(x)$ and $g(x)$ be polynomials. Prove that

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$$

2. Let F be a field. Prove that the ring of polynomials, $F[x]$, is an integral domain.

3. What is the analogue of lemma 20 for integers.

4. Prove proposition 21

5 Polynomials with Integer Coefficients

Definition 23 Let $f(x)$ be a polynomial with integer coefficients. The *, content* of $f(x)$ is the greatest common divisor of the coefficents.

We call $f(x)$ *primitive* if the content is equal to 1.

Given a polynomial $f(x)$ with integer coefficients and content d, we can write $f(x) = dg(x)$, where $g(x)$ is primitive.

Proposition 24 *The product of two primitive polynomials is primitive.*

Proof: Let

$$f(x) = a_0 + a_1x + \cdots + a_mx^m \qquad g(x) = b_0 + b_1x + \cdots + b_nx^n$$

be primitive polynomials. Let p be a prime number.

Since the polynomial $f(x)$ is primitive, we can find the first coefficent, a_i, where p is not a factor. Since the polynomial $g(x)$ is primitive, we can find the first coefficent, b_j, where p is not a factor.

Let $k = i + j$. The polynomial $f(x)g(x)$ has x^k-coefficient

$$c_k = a_ib_j + (a_0b_k + \cdots + a_{i-1}b_{j+1}) + (b_0a_k + \cdots + b_{j-1}a_{i+1})$$

The prime p is a factor of $a_0, \ldots, a_{i-1}$, and of $b_0, \ldots, b_{j-1}$, and is not a factor of a_i or b_j. Hence the prime p is not a factor of the coefficient c_k in the product $f(x)g(x)$.

Thus no prime number is a divisor of all of the coefficients of the product $f(x)g(x)$. Thus the product $f(x)g(x)$ is primitive, and we are done. □

Following the comment proceeding the above proposition, we have the following corollary.

Corollary 25 *Let $f(x)$ and $g(x)$ be two polynomials with integer coefficients and contents d and e respectively. Then the product $f(x)g(x)$ has content de.* □

Lemma 26 (Gauss' Lemma) *Let $f(x)$ be a primitive polynomial. Suppose that $f(x)$ is a product of two polynomials with rational coefficents. Then $f(x)$ is a product of two polynomials with integer coefficients, with the same degrees as those of the rational polynomials.*

Proof: We can write

$$f(x) = \frac{a}{b}u(x)v(x)$$

where $u(x)$ and $v(x)$ are primitive polynomials, and $a \in \mathbb{Z}, b \in \mathbb{N}^{>0}$.

Then $bf(x) = af(x)$. The product $bf(x)$ has content b since the polynomial $f(x)$ is primitive. By proposition 24, the product $u(x)v(x)$ is primitive, so the product $bu(x)v(x)$ has content b.

Therefore $a = b$, meaning $a/b = 1$, and we are done. □

Theorem 27 (Eisenstein Criterion) *Let*

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

be a polynomial with integer coefficients. Suppose that we have a prime number, p, which is a factor of the coefficients $a_0, \ldots, a_{n-1}$, but not a factor of the coefficient a_n, and that p^2 is not a factor of the coefficient a_0.

Then the polynomial $f(x)$ is irreducible over the rational numbers.

Proof: Without loss of generality, assume that $f(x)$ is primitive. Suppose that $f(x)$ factors as a product of two rational polynomials of degree greater than or equal to one. Then by Gauss' lemma, the polynomial $f(x)$ can be expressed as a product of two polynomials

$$b_0 + b_1x + \cdots + b_rx^r$$

and

$$c_0 + c_1x + \cdots + c_sx^s$$

where the coefficents are integers, and $r, s > 0$.

We can see that $a_0 = b_0c_0$, and p but not p^2 is a factor of either b_0 or c_0, but not both. Without loss of generality, suppose that p is a factor of b_0, but not of c_0.

Suppose that all of the coefficients b_i are divisible by p. Then all of the coefficients of the polynomial $f(x)$ are divisible by p, which is false by hypothesis. We can therefore find the first coefficient, b_k, where p is not a factor.

We know

$$a_k = b_k c_0 + b_{k-1} c_1 + \cdots + b_0 c_k$$

Certainly $k < n$, so p is a factor of a_k, and of $b_{k-1}, \ldots, b_0$. However, p is not a factor of b_k or c_0, and so not a factor of the product $b_k c_0$. This l;ast statement is a contradiction.

Hence $f(x)$ cannot be expressed as a product of two rational polynomials of degree greater than or equal to one, and so is irreducible over $\mathbb{Q}$. □

Exercises

1. Give a direct proof of corollary 25.
2. Let p be a prime number. Prove that the polynomial $x^n - p$ is irreducible over the rationals.
3. Prove that the polynomial $1 + x + \cdots + x^{p-1}$, where p is a prime, is irreducible over the rationals. [Hint: Consider the polynomial

   $$1 + (x + 1_) + \cdots + (x + 1)^{p-1}$$

   and use the Eisenstein criterion.
4. Let $a \in \mathbb{Q}$. Suppose that the polynomial $x - a$ divides an integer polynomial with highest coefficient 1. Prove that $a \in \mathbb{Z}$.

6 Algebraic Elements

Given a field extension $F < E$, and a polynomial $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ over the field F, we have a function $p\colon E \to E$ defined by the formuala

$$y \mapsto a_n y^n + a_{n-1} y^{n-1} + \cdots + a_0$$

An element $a \in E$ is termed a *root* of the polynomial $p(x)$ if $p(a) = 0$.

Definition 28 Let $F < E$ be a field extension. Then we call an element $a \in E$ *algebraic* with respect to F if there is a polynomial $p(x) \in F[x]$ such that $p(a) = 0$.

Proposition 29 *Let E be an extension of a field F, and let $a \in E$ be algebraic with repect to F. Then there is a unique polynomial, $p(x)$, of lowest possible degree such that $p(a) = 0$ and the highest coefficient is 1.*

The polynomial $p(x)$ is reducible, and is a factor of any polynomial $q(x)$ such that $q(a) = 0$.

Proof: Since the element a is algebraic, we can find a polynomial $p(x)$ of lowest possible degree such that $p(a) = 0$ and the highest coefficient is 1. Let $q(x) \in F[x]$ be another polynomial such that $q(a) = 0$. Then by the division algorithm

$$q(x) = p(x)m(x) + r(x)$$

where $\deg r(x) < \deg p(x)$.

Since $p(a) = 0$ and $q(a) = 0$, $r(a) = 0$. Hence $r(x) = 0$, otherwise we would contradict the fact that $p(x)$ has the smallest possible degree such that $p(a) = 0$. Hence

$$q(x) = p(x)m(x)$$

so $p(x)$ is a factor of $q(x)$, which proves the last statement of the theorem.

Suppose $\deg q(x) = \deg p(x)$. Then the polynomial $m(x)$ is a constant, C, and

$$q(x) = Cp(x)$$

The polynomial $p(x)$ has highest coefficient 1. If the polynomial $q(x)$ also has highest coefficient 1, then $q(x) = p(x)$, and the polynomial $p(x)$ is the unique polynomial with the stated properties.

Suppose $p(x) = f(x)g(x)$, where $\deg f(x) \geq 1$ and $\deg g(x) \geq 1$. Then $\deg f(x) < \deg p(x)$, and $\deg g(x) < \deg p(x)$. Further, $p(a) = 0$, so $f(a) = 0$ or $g(a) = 0$, which contradicts the polynomial $p(x)$ being of lowest possible degree such that $p(a) = 0$. Hence $p(x)$ is irreducible, and we are done. □

Definition 30 Let E be an extension of a field F, and let $a \in E$ be algebraic with repect to F. Let n be the lowest possible degree of a unique polynomial such that $p(a) = 0$. Then we say that a is *algebraic of degree* n.

Proposition 31 *Let E be an extension of a field F, and let $a \in E$ be a root of an irredicible polynomial in $F[x]$ of degree n. Then a is algebraic of degree n.*

Proof: Suppose that a is algebraic of degree k, where $k < n$. Let $q(x)$ be an irreducible polynomial of degree n such that $p(a) = 0$, and let $p(x)$ be an irreducible polynomial of degree k such that $p(a) = 0$. By the division algorithm

$$q(x) = p(x)m(x) + r(x)$$

where $\deg r(x) < \deg p(x)$.

Since the polynomial $q(x)$ is irreducible, $r(x) \neq 0$. But $r(a) = 0$ since $p(a) = 0$ and $q(a) = 0$, and $r(x)$ has degree less than k, which contradicts the definition of the element a being algebraic of degree k.

Hence $k = \deg(a) \geq n$. Since a is the root of a polynomial of degree n, the definition of the degree tells us that $k = n$, and we are done. □

The main aim of this section is to prove the following important result.

Theorem 32 *Let E be an extension of a field F, and let $a \in E$ be algebraic of degree n. Then* $\deg(F[a]/F) = n$. □

To prove this, we will show that the field $F[a]$ is isomorphic to another field which obviously has degree n.

Proposition 33 *Let E be an extension of a field F, and let $a \in E$ be algebraic of degree n. Then the set*

$$E_a = \{f(a) \mid f(x) \in F[x],\ \deg f(x) < n\}$$

is a subring of E, and is isomorphic to the subring

$$F_0[a] = \{f(a) \mid f(x) \in F[x]\}$$

Proof: The set E_a is clearly closed under addition. Let $p(x) \in F[x]$ be a polynomial of degree n such that $p(a) = 0$. Let $f(x)$ be any polynomial. Then there is a polynomial, $r(x)$, of degree less than n such that

$$f(x) = m(x)p(x) + r(x)$$

Observe $f(a) = r(a)$, and we have a bijection between the set E_a and the subring $F_0[a]$ that preserves addition and multiplication. Thus the set E_a is also a ring, and we are done. □

Proposition 34 *Let $f(x) \in F[x]$ be a polynomial of degree less than n. Let*

$$\theta = f(a) = c_0 + c_1 a + \cdots + c_{n-1}a^{n-1}$$

Then the coefficents c_i are uniquely determined by the element $\theta \in E_a$.

Proof: Suppose

$$\theta = c'_0 + c'_1 a + \cdots + c'_{n-1}a^{n-1}$$

Let $g(x) \in F[x]$ be the polynomial with coefficients c'_i. Then $g(a) = \theta$. Thus $f(a) - g(a) = 0$.

But $f(x) - g(x)$ is a polynomial of degree less than n, and $f(a) - g(a) = 0$. This statement is a contradiction unless $f(x) - g(x) = 0$, that is to say $f(x) = g(x)$, and the coefficients are completely determined. □

We aim to show that the ring E_a is a field isomorphic to the field $F[a]$. The hard part is to prove that the ring E_a is a field. We begin with a reformulation of the definition.

Proposition 35 *Let $p(x)$ be the unique polynomial of degree n with highest coefficient 1 such that $p(a) = 0$.*

Let E_p be the set of formal expressions

$$f(\xi) = c_{n-1}\xi^{n-1} + \cdots + c_1\xi + c_0$$

where

$$f(x) = c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in F[x]$$

Given elements $f(\xi)$ and $g(\xi)$ in E_1, write

$$f(x)g(x) = m(x)p(x) + r(x)$$

where $\deg r(x) < n$, and write $f(\xi) \times g(\xi) = r(\xi)$.

Then E_p is a ring, with addition defined as for polynomials, and multiplication $\times$.

Define addition of elements of E_p as for polynomials, and multiplication $\times$. Then E_p is a ring isomorphic to the ring E_a.

Proof: We can define a map $\alpha\colon E_p \to E_a$ by the formula

$$\alpha(f(\xi)) = f(a)$$

The map α is injective by proposition 34 and surjective by proposiition 33. The bijection α clearly maps the addition defined on the set E_p to the addition of the ring E_a.

Let $f(\xi), g(\xi) \in E_p$. Then $f(\xi) \times g(\xi) = r(\xi)$, where

$$f(x)g(x) = m(x)p(x) + r(x)$$

and $\deg r(x) < n$. Hence

$$f(a)g(a) = m(a)p(a) + r(a) = r(a) = \alpha(r(\xi))$$

so the map α maps the multiplication defined on the set E_p to the multiplication of the ring E_a.

Therefore E_p is a ring isomorphic to the ring E_a, and we are done. □

Proposition 36 *The ring E_p is a field.*

Proof: Let $g(\xi) \neq 0$ and $h(\xi)$ be elements of the field E_p. To show that E_p is a field, we must find $X(\xi) \in E_p$ such that

$$g(\xi) \times X(\xi) = h(\xi)$$

Write

$$h(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$$

and

$$X(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$$

Then

$$g(\xi) \times h(\xi) = L_0(c_0, \ldots, c_{n-1}) + L_1(c_0, \ldots, c_{n-1})x + L_{n-1}(c_0, \ldots, c_{n-1})x^{n-1}$$

where L_i is a linear expression in the coefficents $c_0, \ldots, c_{n-1}$ depending on the polynomial $g(x)$. Hence we need to solve the system of linear equations

$$\begin{array}{rcl} rclL_0(c_0, \ldots, c_{n-1}) & = & b_0 \\ \vdots & & \vdots \\ L_{n-1}(c_0, \ldots, c_{n-1}) & = & b_{n-1} \end{array}$$

The above system of equations is solvable if and only if the corresponding homogeneous system

$$\begin{array}{rcl} rclL_0(c_0, \ldots, c_{n-1}) & = & 0 \\ \vdots & & \vdots \\ L_{n-1}(c_0, \ldots, c_{n-1}) & = & 0 \end{array}$$

has only the trivial solution, that is to say if we have an element $X(\xi) \in E_p$ such that

$$g(\xi) \times X(\xi) = 0$$

then $X(\xi) = 0$. The above equation tells us that

$$g(x)X(x) = m(x)p(x)$$

for some polynomial $m(x)$. By proposition 20, the above equation only holds when $X(x) = 0$, and we are done. $\square$

We now have the technology to prove theorem 32, or rather, a slight refinement.

Theorem 37 *Let E be an extension of a field F, and let $a \in E$ be algebraic of degree n. Let $F[a]$ be the extension generated from F by the element a. Then*

$$F[a] = \{f(a) \mid f(x) \in F[x],\ \deg f(x) < n\}$$

and $\deg(F[a]/F) = n$.

Proof: The field $F[a]$ is the smallest extension of F that contains the element a, and consists of all quotients of polynomials in the element a.

The subset

$$E_a = \{f(a) \mid f(x) \in F[x],\ \deg f(x) < n\}$$

of E is a subfield of E by proposition 36 and proposition 35. The subfield E_a is an extension of E containing a, and is a subfield of the extension $F[a]$.

Since $F[a]$ is the smallest extension of F that contains the element a, it follows that $F[a] = E_a$. By proposition 34, $\deg(E_a/F) = n$, and we are done. $\square$

Corollary 38 *Let $\sigma\colon F \to F'$ be an isomorphism of fields, and let $\sigma_*\colon F[x] \to F'[x]$ be the corresponding isomorphism of polynomial rings coming from applying the isomorphism σ to each coefficient.*

Let $p(x) \in F[x]$ be an irreducible polynomial, and let $p'(x) = \sigma_* p(x) \in F'[x]$. Suppose we have extensions $E = F[\beta]$ and $E' = F'[\beta']$ respectively, where $p(\beta) = 0$ and $p'(\beta') = 0$. Then the isomorphism σ extends to an isomorphism between E and E'.

Proof: Let $n = \deg p(x) = \deg p'(x)$. By theorem 37, the fields E and E' are isomorphic to the fields

$$E_\beta = \{q(\beta) \mid q(x) \in F[x],\ \deg q(x) < n\}$$

and

$$E'_{\beta'} = \{q'(\beta) \mid q'(x) \in F'[x],\ \deg q'(x) < n\}$$

respectively.

By proposition 34, the isomorphism σ extends to an isomorphism for E_β to $E'_{\beta'}$. $\square$

Theorem 39 (Kronecker) *Let $p(x)$ be a polynomial over a field F. Then there is an extension, E, where $p(x)$ has a root. Further, if $p(x)$ is irreducible with degree n, then* $\deg(E/F) = n$.

Proof: Without loss of generality, let $p(x)$ be irreducible, with degree n; if $p(x)$ is not irreducible, we can choose an irreducible factor, and a root of that factor is also a root of the original polynomial.

By proposition 36, we have an extension, E_p, of F, of degree n, defined as in proposition 35.

Write

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n$$

so

$$a_n x^n - p(x) = -a_0 - a_1 x - \cdots - a_{n-a} x^{n-1}$$

Using the definition of multiplication in the field E_p,

$$a_n \xi^n = -a_0 - a_1 \xi - \cdots - a_{n-a} \xi^{n-1}$$

so $p(\xi) = 0$, so ξ is a root of $p(x)$ in the extension E_p, and we are done. □

Exercises

1. Let E be a finite extension of a field F. Prove that every element of E is algebraic.
2. It is true that every infinite extension of a field contains non-algebraic elements.
3. Prove proposition 31 as a corollary to proposition 29.
4. Find $\deg(\mathbb{Q}[\sqrt{2}], \mathbb{Q})$.
5. Find $\deg(\mathbb{Q}(2^{1/3}), \mathbb{Q})$.
6. Let E be an extension of a field F. Prove that the set of algebraic elements of E with respect to F is a subfield of E.

7 Transcendence of e

Definition 40 A real number $x \in \mathbb{R}$ is called *transcendental* if it is not the root of a polynomial with integer coefficients.

To rephrase the above definition slightly, a real number is transcendental if and only if it is not algebraic with respect to $\mathbb{Q}$.

A transcendental number is clearly irrational.

As the title of this section indicates, the main purpose is to give a direct proof that the number e is transcendental. This proof uses only some elementary applications of the exponential function and the mean value theorem from differential calculus.

We begin by stating a few lemmas. The proofs of the first two are left as exercises.

Lemma 41 *Let $g(x)$ be a polynomial with integer coefficients. Let p be a prome number. Then, for $i \geq p$, the expression*

$$\frac{d}{dx^1}\left(\frac{g(x)}{(p-1)!}\right)$$

is a polynomial with integer coefficients divisible by p. □

Lemma 42 *Let $a \in \mathbb{R}$. Then*

$$\lim_{n\to\infty} \frac{a^n}{n!} = 0$$

□

Lemma 43 *Let $n \in \mathbb{N}$, and let $p > n$ be a prime number. Let*

$$f(x) = \frac{1}{(p-1)!}x^{p-1}(1-x)^p(2-x)^p\cdots(n-x)^p$$

be the Hermite polynomial*, and let $r = np + p - 1$ be the degree of $f(x)$.*

Let $f^{(n)}(x)$ denote the n-th derivative of $f^{(n)}(x)$, and write

$$F(x) = f(x) + f^{(1)}(x) + \cdots + f^{(r)}(x)$$

Let $j \in \{1, 2, \ldots, n\}$. Then $F(j)$ is an integer multiple of p. The number $F(0)$ is an integer, but not an integer multiple of p.

Proof: We can write

$$f(x) = \frac{n!}{(p-1)!}x^{p-1} + \frac{a_0x^p}{(p-1)!} + \frac{a_1x^{p+1}}{(p-1)!} + \cdots + \frac{a_{np-1}x^{p+np-1}}{(p-1)!}$$

where $a_i \in \mathbb{Z}$.

By lemma 41, the coefficients of the polynomial $f^{(i)}(x)$ are integer multiples of p when $i \geq p$. By definition, $f(x)$ has a root of multiplicity p at $x = 1, 2, \ldots, n$, and

$$f(j) = f^{(1)}(j) = \cdots = f^{(p-1)}(j) = 0$$

when $j \in \{1, \ldots, n\}$, so

$$F(j) = f^{(p)}(j) + \cdots + f^{(r)}(j)$$

is an integer multiple of p.

By definition, $f(x)$ has a root of multiplicity $p-1$ at $x = 0$. Therefore

$$f(0) = f^{(0)}(j) = \cdots = f^{(p-2)}(0) = 0$$

Observe $f^{(p-1)}(0) = (n!)^p$, and as before, $f^{(i)}(0)$ is an integer multiple of p when $i \geq p$. Since p is a prime number, and $p > n$, p is not a factor of $(n!)^p$. Hence $F(0)$ is an integer, but not an integer multiple of p. □

Theorem 44 *The number e is transcendental.*

Proof: Let $f(x)$ be a real polynomial of degree r. Taking derivatives, let

$$F(x) = f(x) + f^{(1)}(x) + \cdots + f^{(r)}(x)$$

Since the polynomial $f(x)$ has degree r, $f^{(r+1)}(x) = 0$. Now

$$\frac{d}{dx}(e^{-x}F(x)) = -e^{-x}F(X) + e^{-x}(F(x) - f(x)) = -e^{-x}f(x)$$

Let $k \in \mathbb{N}$. By the mean value theorem, we can find $\theta_k \in (0,1)$ such that

$$\frac{e^{-k}F(k) - e^{-0}F(0)}{k} = -e^{-\theta_k k}f(\theta_k k)$$

that is to say

$$F(k) - e^k F(0) = -ke^{(1-\theta_k)k}f(\theta_k k)$$

Supppose that e is not a transcendental number. Then we can find a polynomial, $p(x)$, with integer coefficients such that $p(e) = 0$. Write

$$p(x) = c_0 + c_1 x + \cdots + c_n x^n$$

We can assume without loss of generality that $c_0 > 0$. Define

$$\epsilon_k = e^{-\theta_k k}f(\theta_k k)$$

Taking the above equation for $F(k)$ and multiplying by c_k for $k = 1, \ldots, n$, we see

$$\begin{aligned} c_1(F(1) - eF(0)) &= -c_1\epsilon_1 \\ &\vdots \quad\quad \vdots \\ c_n(F(n) - e^n F(0)) &= -c_n\epsilon_n \end{aligned}$$

Adding:

$$c_1F(1) + \cdots + c_nF(n) - (p(e) - c_0)F(0) = -c_1\epsilon_1 - \cdots - c_n\epsilon_n$$

Since $p(e) = 0$:

$$c_0F(0)c_1F(1) + \cdots + c_nF(n) = -c_1\epsilon_1 - \cdots - c_n\epsilon_n$$

Now, let $f(x)$ be the Hermite polynomial for a number n and prime number $p > n$ from lemma 43. Suppose further that $p > c_0$. Then p is not a factor of c_0. By lemma 43, the prime p is not a factor of $F(0)$, but is a factor of $F(1), \ldots, F(n)$. Hence the sum

$$c_0F(0)c_1F(1) + \cdots + c_nF(n)$$

is an integer and is not divisible by p. By the above equation, the sum

$$c_1\epsilon_1 + \cdots + c_n\epsilon_n$$

is thus also an integer that is not divisible by p.

Recall

$$\epsilon_k = ke^{(1-\theta_k)k}f(\theta_k k) \qquad \theta_k \in (0,1)$$

By definition of the Hermite polynomial

$$\epsilon_k = ke^{(1-\theta_k)k} \frac{(1-k\theta_k)^p(2-k\theta_k)^p \cdots (n-k\theta_k)^p (k\theta_k)^{p-1}}{(p-1)!}$$

so

$$|\epsilon_k| \leq \frac{e^{k(n!)^p k^p}}{(p-1)!} \leq \frac{e^p (n!)^p n^p}{(p-1)!}$$

since the exponential function is monotonic increasing.

By lemma 42

$$\lim_{p\to\infty} \frac{e^p (n!)^p n^p}{(p-1)!} = 0$$

Thus we can find a prime number p which is large enough that

$$|c_1\epsilon_1 + \cdots + c_n\epsilon_n| < 1$$

Since this expression is an integer, we conclude that

$$c_1\epsilon_1 + \cdots + c_n\epsilon_n = 0$$

However, we know that the prime p is not a factor of the above expression. The prime p is certainly a factor of p. This statement is a contradiction of the one assumption we made, namely that the number e is not transcendental. □

Exercises

1. Prove that the set of real numbers which are algebraic over $\mathbb{Q}$ is countable. Deduce that transcendental numbers exist.
2. Use the formula
$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots$$
to give a direct proof that the number e is irrational.
3. Prove lemma 41.
4. Prove lemma 42.
5. Let $q \in \mathbb{Q}\backslash\{0\}$. Prove that the number e^q is transcendental.

8 Factorisations of Polynomials

In this section we investigate the connection between the roots of a polynomial and its factors.

Proposition 45 *Let F be a field, and let $p(x) \in F[x]$. Let $a \in F$ be a root of $p(x)$. Then the polynomial $x - a$ is a factor of $p(x)$.*

Proof: The degree of the polynomial $p(x)$ is 1. Hence, by the division algorithm, we can write

$$p(x) = m(x)(x - a) + C$$

where $C \in F$ is a constant (that is a degree 0 polynomial). Since $p(a) = 0$ and $a - a = 0$, we see that $C = 0$, so

$$p(x) = m(x)(x - a)$$

and we are done. □

Corollary 46 *Let $p(x) \in F[x]$ be a degree n polynomial. Then $p(x)$ has at most n roots.*

Proof: Let $a_1, \ldots, a_k$ be the roots of $p(x)$. Then by the above proposition, the polynomial $p(x)$ must be divisible by the product

$$(x - a_1) \cdots (x - a_k)$$

which must have degree at most n. Hence $k \leq n$, and we are done. □

Theorem 47 *Let F be a field, and let $p(x) \in F[x]$. Suppose*

$$p(x) = f_1(x) \cdots f_r(x) = g_1(x) \cdots g_s(x)$$

are two factorisations into irreducible polynomials of degree at least one. Then $r = s$, and up to a change in the order of the $g_j(x)$, there are constants $c_i \in F$ such that $p_i(x) = c_i q_i(x)$ for all i.

Proof: For the sake of convenience, suppose the leading coefficients of the factors $p_i(x)$ and $g_j(x)$ are all 1.

By the Kronecker theorem, we can find an extensions, E, of F, and an element $a \in E$ such that $f_1(a) = 0$. Hence $p(a) = 0$, and at least one of the $g_j(a) = 0$. Reorder so that $g_1(a) = 0$.

By proposition 31, the element x has degree $\deg f_1(x) = \deg g_1(x)$. By proposition 29, it follows that $f_1(x) = g_1(x)$. Hence

$$f_2(x) \cdots f_r(x) = g_2(x) \cdots g_s(x)$$

Repeating the above argument, the desired result follows by induction. □

Definition 48 Let $F < B < E$ be a pair of extensions of a field F. Then we call B an *intermediate field* for the extension E.

Definition 49 Let F be a field, and let $p(x) \in F[x]$. An extension, E, of F, where $p(x)$ can be expressed as a product of linear factors (that is, degree 1 polynomials), and $p(x)$ has no such factorisation in any intermediate field is called a *splitting field*, for F.

We say that a polynomial *splits* over an extension if it can be expressed as a product of linear factors in that extension.

The following result is straightforward to prove; the details are left as an exercise.

Proposition 50 *Let $p(x) \in F[x]$ be a polynomial with leading coefficient 1. Let E be a splitting field for $p(x)$. Over the field E, write*

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

Then the roots of the polynomial $p(x)$ are $a_1, \ldots, a_n$. □

Thus, if E is a splitting field for a polynomial $p(x)$, then E is obtained by adjunction of the roots of $p(x)$ in E.

Proposition 51 *Let $p(x) \in F[x]$ be a degree n polynomial. Then a splitting field for $p(x)$ has degree at most $n!$.*

Proof: Let E be a splitting field of the polynomial $p(x)$. Over the field E, write

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

We have a sequence of extensions

$$F < F[a_1] < F[a_1, a_2] < \cdots < F[a_1, \ldots, a_n] = E$$

By theorem 37, the field $F[a_1]$ has degree at most n over F. Define

$$p_i(x) = (x - a_i) \cdots (x - a_n)$$

Then the polynomial $p_i(x)$ has degree $(n - (i - 1))$. The element $a_i \in E$ is a root of the polynomial $p_i(x)$ over the field $F[a_1, \ldots, a_{i-1}(x)]$. Hence by theorem 37,

$$\deg(F[a_1, \ldots, a_i]/F[a_1, \ldots, a_{i+1}]) \leq (n - (i - 1))$$

The desired result now follows by proposition 6. □

By the above corollary, the polynomial $p(x)$ can have at most $\deg p(x)$ roots. Hence, by theorem 37, a splitting field has degree at most n.

Theorem 52 *Let F be a field, and let $p(x) \in F[x]$. Then a splitting field for $p(x)$ exists.*

Proof: Write

$$p(x) = f_1(x) \cdots f_r(x)$$

where the polynomials $f_i(x)$ are irreducible. If each factor $f_i(x)$ has degree 1, then F itself is the required splitting field.

Suppose that $\deg f_1(x) > 1$. Bvy the Kronecker theorem, there is an extension, F_1, of F where $f_1(x)$ has a root, a. Hence, by proposition 45,

$$f_1(x) = (x - a) f_1'(x)$$

over the field F_1, and $\deg f_1'(x) = \deg f_1(x) - 1$.

Repeating this process, we eventually obtain a field E, where $p(x)$ can be split into linear factors.

The field generated from F by the roots of the polynomial $p(x)$ in E is the required splitting field. □

Theorem 53 *Let $\sigma\colon F \to F'$ be an isomorphism of fields, and let $\sigma_*\colon F[x] \to F'[x]$ be the corresponding isomorphism of polynomial rings coming from applying the isomorphism σ to each coefficient.*

Let $p(x) \in F[x]$ be an irreducible polynomial, and let $p'(x) = \sigma_* p(x) \in F'[x]$. Let E be a splitting field of $p(x)$, and let E' be a splitting field for $p'(x)$. Then σ extends to an isomorphism for E to E'.

Proof: If all roots of the polynomial $p(x)$ lie in F, then all roots of the polynomial $p'(x)$ lie in F', so F and F' are respectively the splitting fields for the polynomials $p(x)$ and $p'(x)$, and we are done.

Let $n > 1$. Suppose the result holds whenever the number of roots of the polynomial that do not lie in F is less than n. Let $p(x) \in F[x]$ be a polynomial where n roots of $p(x)$ do not lie in F.

Write

$$p(x) = f_1(x) \cdots f_n(x)$$

where the $f_i(x)$ are irreducible over F. Since $n > 1$, at least one of the polynomials $f_i(x)$ has degree greater than 1; without loss of generality, say $\deg f_1(x) = r > 1$.

Write

$$p'(x) = f'_1(x) \cdots f'_n(x)$$

where $f'_i(x) = \sigma_* f_i(x)$, so $f'_i(x)$ is irreducible over F'.

Let $a \in E$ be a root of $f_1(x)$, and let $a' \in E'$ be a root of $f'_1(x)$. Then by corollary 38, we can extend σ to an isomorphism $\sigma_1\colon F[a] \to F[a']$.

But the polynomial $p(x)$ has less than n roots outside of the field $F[a]$. Hence, by inductive hypothesis, the isomorphism σ_1 extends to an isomorphism between the fields E and E', and we are done. □

Corollary 54 *Let $p(x) \in F[x]$. Then any two splitting fields for $p(x)$ are isomorphic.* □

It therefore makes sense to talk about *the* splitting field of a polynomial, rather than just a splitting field.

Exercises

1. Let $p(x) \in F[x]$ be an irreducible degree n polynomial. Let E be an extension of F, and let $a \in E$ be an element where $p(a) = 0$. Prove that $F[a]$ is a splitting field for $p(x)$.

2. Prove proposition 50

9 Ruler and Compass Constructions

In this section we present a geometric application of the theory we have developed so far.

Definition 55 A *ruler and compass construction* in $\mathbb{R}^2$ is a figure which can be obtained from a certain set of known points by a finite number of the following steps.

- Drawing a line through two known points.
- Drawing a line segment between two known points.
- Drawing a circle with centre on a known point, and boundary on another known point.
- Taking a point from the intesection of two known lines, a known line and a known circle, or two known circles.

There are analogous definitions in higher dimensions. We will generally assume that we begin with two known points. The next result is left as an exercise.

Proposition 56 *A line parallel or perpendicular to a known line through a known point can be obtained by a ruler and compass construction.* □

Definition 57 A real number $\alpha \in \mathbb{R}$ is *constructible* if we can obtain a line segment of length $|\alpha|$ from two points distance 1 apart using a ruler and compass construction.

We write W to denote the set of constructible numbers.

The following result is an application of proposition 56, and is again left as an exercise.

Proposition 58 *The set W is a subfield of the field $\mathbb{R}$. It is an extension of the field $\mathbb{Q}$.* □

For convenience, let us call a figure that can be obtained by a ruler and compass construction from the points $(0,0)$ and $(1,0)$ *constructible*. The next result is easy to check.

Proposition 59 *A line in $\mathbb{R}^2$ can be obtained by a ruler and compass contruction from the points $(0,0)$ and $(1,0)$ if and only if it has the form*

$$\{(x,y) \in \mathbb{R}^2 \mid ax + by + c = 0\}$$

where $a, b, c \in \mathbb{Q}$.

A circle in $\mathbb{R}^2$ can be obtained by a ruler and compass contruction from the points $(0,0)$ and $(1,0)$ if and only if it has the form

$$\{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 + ax + by + c = 0\}$$

where $a, b, c \in \mathbb{Q}$. □

The main point of this section is that certain figures cannot be obtained by a ruler and compass construction.[1]

Theorem 60 *Let $\alpha \in \mathbb{R}$. Then α is constructible if and only if we can find real numbers $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ such that*

- $\lambda_1^2 \in \mathbb{Q}$.
- $\lambda_i^2 \in \mathbb{Q}[\lambda_1, \ldots, \lambda_{i-1}]$ *whenever* $2 \leq i \leq n$.
- $\alpha \in Q[\lambda_1, \ldots, \lambda_n]$

Proof: Let F be a subfield of $\mathbb{R}$. A line through two points in F^2 takes the form

$$\{(x, y) \in \mathbb{R}^2 \mid ax + by + c = 0\}$$

where $a, b, c \in F$. A circle with centre on a point in F^2 passing through another point of F^2 takes the form

$$\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 + ax + by + c = 0\}$$

where again $a, b, c \in F$.

Intersections of lines and circles constructed from points in F^2 thus come from solving quadratic equations with coefficients in F^2. By the quadratic fromula, solutions to such equations lie in the field

$$F[\sqrt{\gamma}] \qquad \gamma \in F,\ \gamma \geq 0$$

It follows that W is the smallest subfield of $\mathbb{R}$ that contains $\mathbb{Q}$ where

$$W[\sqrt{\gamma}] = W \text{ whenever } \gamma \in W,\ \gamma \geq 0$$

The result now follows. □

Corollary 61 *Let $\alpha \in W$. Then α lies in some extension of $\mathbb{Q}$ with degree a power of 2.*

Proof: Let $\alpha \in W$. Then by the above theorem, there are real numbers $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ such that

- $\lambda_1^2 \in \mathbb{Q}$.
- $\lambda_i^2 \in \mathbb{Q}[\lambda_1, \ldots, \lambda_{i-1}]$ whenever $2 \leq i \leq n$.
- $\alpha \in Q[\lambda_1, \ldots, \lambda_n]$

By theorem 37, the degree $\deg(\mathbb{Q}[\lambda_1, \ldots, \lambda_i]/\mathbb{Q}[\lambda_1, \ldots, \lambda_{i-1}])$ is either 1 or 2. By corollary 7, the degree $\deg(\mathbb{Q}[\lambda_1, \ldots, \lambda_n]/\mathbb{Q})$ is a power of 2. □

Corollary 62 *Let $p(x) \in \mathbb{Q}[x]$ be a rational irreducible polynomial of degree k, where k is not a power of 2. Then no root of $p(x)$ is constructible.*

[1] It is of course possible to construct many more figures if other tools are allowed, but that is not the point of the current mathematical exercise.

Proof: Let $p(a) = 0$. By proposition 31, the root a is algebraic of degree k. The smallest extension of $\mathbb{Q}$ containing a is $\mathbb{Q}[a]$, which has degree k by theorem 37. Hence any finite extension of $\mathbb{Q}$ which contains a has degree divisible by k, by proposition 6. It follows that no such extension has degree a power of 2, since k is not a power of 2.

Thus the root a is not constructible, by the above corollary. □

In particular, roots of irreducible cubic equations over $\mathbb{Q}$ are not constructible.

Example 63 We cannot trisect the angle $\pi/3$ by a ruler and compass construction.

To see this, let $\theta = \pi/9$. If the trisection were possible, then the number $\alpha = \cos\theta$ would be in W.

But

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

and $\cos 3\theta = \cos(\pi/3) = 1/2$, so

$$\frac{1}{2} = 4\alpha^3 - 3\alpha$$

that is to say

$$8\alpha^3 - 6\alpha - 1 = 0$$

If we can show that the polynomial

$$p(x) = 8x^3 - 6x - 1$$

is irreducible over $\mathbb{Q}$, then we are done by corollary 62.

Let p/q be a rational solution to the above equation, where $p \in \mathbb{Z}$ and $q \in \mathbb{N}$ have no common factors. Then

$$8\left(\frac{p}{q}\right)^3 - 6\left(\frac{p}{q}\right) - 1 = 0$$

and

$$8p^3 - 6pq^2 - q^3 = 0$$

which means that 2 is always a factor of q^3, and so of q. Write $q = 2k$. Then

$$p^3 - 3pk^2 - k^3 = 0$$

If k is even, we see immediately that p^3 is even. Thus 2 is a factor of p^3, and so of p, which cantradicts p and q having no common factors.

If k is odd, then, as above, p is also odd. Hence $3pk^2$ and k^3 are odd, so $3pk^2 + k^3$ is even. We conclude that p^3, and so p are even, which is is a contradiction.

Hence the polynomial $p(x)$ has not rational roots, and therefore no rational factors of degree 1. Since $p(x)$ has degree 3, it can also have no rational factors of degree 2. Thus $p(x)$ is irreducible, and we are done.

Example 64 We can also look at ruler and compass contructions in $\mathbb{R}^3$, and ask if it is possible to construct a cube with volume twice that of a given cube.

This amounts to finding a constructible solution to the equation $x^3 = 2$. By the Eisenstein criterion, the polynomial $p(x) = x^3 - 2$ is irreducible over $\mathbb{Q}$. Thus, as above, this problem cannot be solved using a ruler and compass construction.

Example 65 Suppose we want to construct a regular septagon. Then we need to construct the angle $2\pi/7$. If this were possible, then the number $\alpha = \cos 2\pi/7$ would be in W.

Let $z = e^{2\pi i/7}$, so α is the real part of z. Then $z^7 = 1$, so $z^7 - 1 = 0$ and

$$(z-1))(1 + z + z^2 + \cdots + z^6) = 0$$

Since $z \neq 1$, we see

$$1 + z + z^2 + \cdots + z^6 = 0$$

Now, using once more the identity $e^{i\theta} = \cos\theta + i\sin\theta$, we see that

$$\Re(z^6) = \Re(z) \qquad \Re(z^2) = \Re(z^5) \qquad \Re(z^3) = \Re(z^4)$$

Hence

$$\Re(1 + 2z + 2z^2 + 2z^3) = 0$$

that is to say

$$1 + 2\alpha + 2\cos(2(2\pi/7)) + 2\cos(3(2\pi/7))$$

Using the identities

$$\cos 2\theta = 2\cos^2\theta - 1 \qquad \cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

we see that

$$8\alpha^3 + 4\alpha^2 - 4\alpha - 1 = 0$$

As above, the polynomial $p(x) = 8x^3 + 4x^2 - 4x = 1$ is irreducible over $\mathbb{Q}$, and the problem cannot be solved with a ruler and compass construction.

Exercises

1. Prove that the set of constructible numbers is countable.
2. Prove proposition 56.
3. Prove proposition 58.
4. Prove proposition 59.
5. Using (without proof) the fact that the number π^2 is transcendental, prove that a ruler and compass construction cannot construct a square with area equal to that of a known circle.
6. Prove that the regular hexagon can be constructed by a ruler and compass construction.

7. Prove that the polynomial

$$p(x) = x^3 - 2$$

is irreducible over $\mathbb{Q}$.

8. Prove that the polynomial

$$p(x) = 8x^3 + 4x^2 - 4x - 1$$

is irreducible over $\mathbb{Q}$.

9. Prove that the regular nine-sided polygon cannot be constructed by a ruler and compass construction.

10. Prove that the regular pentagon can be constructed by a ruler and compass construction.

10 Finite Characteristics

Let F be any field. Let $a \in F$. Then for any natural number n, we define na to be the n-fold sum

$$na = a + \cdots + a \in F$$

Definition 66 The field F is said to have *characteristic* 0 if $na \neq 0$ whenever $a \in F$ and $n \in \mathbb{N}^{>0}$. Otherwise F is said to have *finite characteristic*.

Let F be a field of finite characteristic. Suppose that we have $a \in F \backslash \{0\}$ such that $na = 0$. Let $b \in F$. Then

$$nb = (na)(a^{-1}b) = 0(a^{-1}b) = 0$$

The following definition therefore makes sense.

Definition 67 If F has finite characteristic, the *characteristic* is defined to be the smallest natural number $n \in \mathbb{N}^{>0}$ such that $na = 0$ for all $a \in F$.

Clearly any finite field has finite characteristic.

Proposition 68 *Let F have finite characteristic. Then the characteristic of F is a prime number.*

Proof: Let p be the characteristic of F. Suppose that $p = rs$, where r and s are integers greater than one. Then

$$p1 = r(s1) = 0$$

Write $b = s1$. Suppose that $b \neq 0$. Let $a \in F$. Then

$$ra = rb(b^{-1}a) = r(s1)(b^{-1}a) = 0$$

so p has characteristic $r < p$, which is a contradiction.

Hence $s1 = 0$, which as above implies that the field F has characteristic $s < p$, again a contradiction. Therefore p must be a prime number. □

Proposition 69 *Let F be a finite field with q elements. Let E be an extension of F with degree $\deg(E/F) = n$. Then E has q^n elements.*

Proof: Let $\{e_1, \ldots, e_n\}$ be a basis of E considered as a vector space over the field F. Then

$$E = \{a_1 e_1 + \cdots + a_n e_n \mid a_i \in F\}$$

By linear independence of a basis, the coefficients $a_i \in F$ are uniquely determined by the sum $a_1 e_1 + \cdots + a_n e_n \mid a_i \in F\}$. Since the field F has q elements, we see that the field E has q^n elements. □

Proposition 70 *Let F be a finite field. Let p be the characteristic of F. Then F has p^n elements for some n.*

Proof: Let

$$P = \{0, 1, 2 \ldots, p-1\}$$

be the set of multiples of the identity element of the field F. Then P is a subfield of F.

The subfield P has p elements, and since the field F is finite, it is a finite extension of the field P. By the above proposition, the field F has p^n elements, where $n = \deg(F/P)$. □

Theorem 71 *Two finite fields with the same number of elements are isomorphic.*

Proof: Let F and F' be finite fields with the same number of elements. By the above results, any finite field has a number of elements equal to some power of its characteristic, and the characteristic of a field is a prime number.

Hence, both F and F' have $q = p^n$ elements, where p is a prime number. Let $F^\times$ be the set of non-zero elements of the field F, and $F'^\times$ be the set of non-zero elements of the field F'. The sets $F^\times$ and $F'^\times$ are abelien groups, each with $q-1$ elements, under the operation of multiplication in their respective fields.

Any element of the group $F^\times$ or $F'^\times$ thus has order that divides $q-1$. Hence

$$x^{q-1} - 1 = 0$$

whenever x is a non-zero element of one of the two fields.

Let

$$P = \{0, 1, 2 \ldots, p-1\}$$

be the set of multiples of the identity element of the field F, and P' the set of multiples of the identity element of the field F'. Then the fields P and P' are isomorphicin the obvious, and the polynomial $f(x) = x^{q-1} - 1$ can be considered to be over the field P or P', and is preserved by the obvious isomorphism between these fields.

The polynomial $f(x)$ is of degree $q-1$, and so has at most $q-1$ roots in any extension of the field P. In the extension F of the field P, the polynomial $f(x)$ has precisely $q-1$ roots. Hence F is a splitting field of $f(x)$ over P.

Similarly, F' is a splitting field of $f(x)$ over P'. Hence F and F' are isomorphic by theorem 53, and we are done. □

Before stating our last result on the structure of finite theorems, we will state without proof a few results from the theory of abelian groups.

Lemma 72 *Let G be an abelian group. Let $x, y \in G$ be elements of order m and n respectively. Then G contains an element with order the lowest common multiple of m and n.* □

Lemma 73 *Let G be an abelian group. Suppose that G contains an element of maximal order. Then the order of every finite order element is a factor of c.* □

We are now ready for our main result.

Theorem 74 *Let F be a field, and let S be a finite subset of F which is a group under the operation of multiplication in F. Then S is a cyclic group.*

Proof: Let $n = |S|$. Let r be the largest order of an element of S. Then by lemma 73, $x^r - 1 = 0$ for all $r \in S$.

Now the equation $x^r - 1 = 0$ has at most r roots. On the other hand, each of the n elements of the group S is a root. Therefore $r \geq n$.

By Lagrange's theorem for finite groups, the order of every element of the group S is a factor of n. Therefore $r \leq n$. Thus $r = n$, and S is the cyclic group with n elements. □

Exercises

1. Why is the the product of two fields not in general a field?
2. Prove that any finite field has finite characteristic.
3. Let G be a group with p elements, where p is a prime number. Prove that G is the cyclic group, with order p.
4. Prove lemma 72.
5. Prove lemma 73
6. Let F be a finite field with p elements, where p is a prime number. Describe the structure of F.
7. Let F be a finite field with p^n elements, where p is a prime number. Describe the structure of F.
8. Let F be a finite field, and let E be a finite extension. Prove that $E = F(a)$ for some element $a \in F$.

11 Derivatives and Roots

Definition 75 Let

$$f(x) = a_0 + a_1 x + \cdots a_n x^n$$

be a polynomial over a field F. Then we define the *derivative* of $f(x)$ to be the polynomial

$$f'(x) = a_1 + 2a_2 x + 3a_3 x^2 + \cdots n a_n x^{n-1}$$

Note that the above definition does not need any analysis, but does agree with the analytic formula for the derivative of a polynomial in cases where the latter notion makes sense.

Example 76 Let F be a field of characteristic p. Let $f(x) = x^p$. Then $f'(x) = px^{p-1} = 0$. Thus non-constant polynomials can have zero derivatives in a field of finite characteristic.

Proposition 77 *Let F be a field. Let $f(x), g(x) \in F[x]$, and let $C \in F$. Then*

- $(f(x) + g(x))' = f'(x) + g'(x)$
- $(Cf(x))' = Cf'(x)$
- $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$
- $(f(x)^n)' = nf(x)^{n-1}f'(x)$

□

We have already seen that if a is a root of a polynomial $f(x)$, than $x - a$ is a factor.

Definition 78 Let $f(x) \in F[x]$. A root $a \in F$ is said to hvae *multiplicity* k if $(x-a)^k$ is a factor of $F[x]$, but $(x-a)^{k+1}$ is not a factor of $F[x]$.

A root of multiplicity at least 2 is termed a *repeated root*. A polynomial is termed *separable* if its irreducible factors do not have repeated roots.

Thus a polynomial of order n has precisely n roots over its splitting field, provided we count the multiplicity of each root.

Theorem 79 *Let $f(x) \in F[x]$. The polynomial $f(x)$ has a multiple root over its splitting field if and only if the polynomial $f(x)$ and derivative $f'(x)$ have a non-trivial common factor.*

Proof: Let E be the splitting field of $f(x)$. Let $a \in E$ be a root of $f(x)$ with multiplicity $k \geq 2$. Then

$$f(x) = (x-a)^k q(x)$$

for some polynomial $q(x)$. It follows by proposition 77 that

$$f'(x) = k(x-a)^{k-1}q(x) + (x-a)^k q'(x)$$

It follows that $x - a$ is a common factor of $f(x)$ and $f'(x)$ over the splitting field. Hence, by corollary 22, the polynomials $f(x)$ and $f'(x)$ have a common factor over the original field.

Conversely, suppose that the polynomials $f(x)$ and $f'(x)$ have a common factor. Then they have a common factor of the form $x - a$ over the splitting field. Write

$$f(x) = (x - a)k(x)$$

Then by proposition 77

$$f'(x) = (x - a)k'(x) - ak(x)$$

By hypothesis, the polynomial $x - a$ is a factor of the derivative $f'(x)$. Thus $x - a$ is a factor of the polynomial $k(x)$. Write $k(x) = (x - a)g(x)$. Then

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

and we see that a is a multiple root of the polynomial $f(x)$. □

Corollary 80 *Let F be a field of characteristic zero. Then every irreducible polynomial over F is separable.*

Proof: Let $f(x) \in F[x]$. Suppose that $f(x)$ has a multiple root over the splitting field. Then $f(x)$ and $f'(x)$ have a non-trivial common factor. Since $f'(x) \neq 0$, the polynomial $f(x)$ has a non-trivial factor. Hence $f(x)$ is not irreducible.

Thus no non-separable polynomial can be irreducible. □

Corollary 81 *Let F be a field of characteristic $p \neq 0$. Let $f(x) \in F[x]$ be an irreducible polynomial. Then $f(x)$ has a multiple root if and only if $f(x) = g(x^p)$ for some polynomial $g(x)$.*

Proof: Suppose that $f(x) = g(x^p)$. Then $f'(x) = px^{p-1}g(x^p) = 0$ since F has characteristic p. Therefore $f(x)$ and $f'(x)$ have a non-trivial common factor, namely $f(x)$, and the polynomial $f(x)$ has multiple roots.

Conversely, suppose $f(x)$ is irreducible, and has multiple roots. Then by the above argument, $f'(x) = 0$. As proved in the exercises, the only way this can occur is when $f(x) = g(x^p)$ for some polynomial p. □

Example 82 Let F_2 be the field with two elements. Let $F = F_2(x)$. Then the field F hs characteristic 2. Define a polynomial $p(t) = t^2 - x \in F[t]$.

Suppose that $f(x)$ is a rational function in F_2. Write $f(x) = g(x)/h(x)$ where $g(x)$ and $h(x)$ have no non-constant common factors. Suppose that $f(x)^2 = x$. Then

$$x^2 = \frac{g(x)^2}{h(x)^2}$$

and

$$g(x)^2 = xh(x)^2$$

so x is a factor of $g(x)^2$, and therefore a factor of $g(x)$. Write $g(x) = xk(x)$. Then

$$x^2 k(x)^2 = xh(x)^2$$

and

$$xk(x) = h(x)^2$$

so x is a factor of $h(x)^2$, and therefore a factor of $h(x)$. So the polynomials $g(x)$ and $h(x)$ must have a common factor, which is a contradiction.

We conclude that there is no rational function $f(x)$ such that $f(x)^2 = x$. Therefore the polynomial

$$p(t) = t^2 - x \in F[t]$$

is irreducible.

Now

$$p'(t) = 2t = 0$$

since the field F has characteristic 2. Hence the polynomial $p(t)$ and the root $p'(t)$ have a non-trivial common factor, $p(t)$, so the polynomial $p(t)$ has a multiple root ove its splitting field and is therefore not separable.

Exercises

1. Let F be a field of characteristic 0. Let $f(x) \in F[x]$, and suppose that $f'(x) = 0$. Prove that $f(x)$ is constant.
2. Prove proposition 77
3. Let F be a field of characteristic p. Suppose that $f'(x) = 0$. Prove that there is a polynomial $g(x)$ such that $f(x) = g(x^p)$.
4. Let F be a field of characteristic p. Prove that the polynomial

   $$x^{p^n} - x$$

   has p^n distinct roots.
5. Prove corollary 105.

12 Group Characters and Fixed Points

Let F be a field. Then we write $F^\times$ to denote the group of all non-zero elements of F, equipped with the operation of multiplicaition.

Definition 83 Let G be a group. Then a *character* of G in a field F is a group homomorphism $\omega\colon G \to F^\times$.

The following definition is analagous to linear algebra.

Definition 84 Let $\omega_1, \ldots, \omega_n\colon G \to F^\times$ be characters of a group G. Then we call $\omega_1, \ldots, \omega_n$ *independent* if whenever there are elements $a_1, \ldots, a_n \in F$ such that

$$a_1\omega_1(g) + \cdots + a_n\omega_n(g) = 0$$

for all $g \in G$, then $a_i = 0$ for all i.

The following result, however, has no analogue in linear algebra.

Proposition 85 *Let $\omega_1, \ldots, \omega_n$ be distinct characters of a group G in a field F. Then the characters $\omega_1, \ldots, \omega_n$ are independent.*

Proof: We proceed by induction on the size of the set of characters. To begin with, if $\omega\colon G \to F^\times$ is a single character, then $\omega(g) \neq 0$ for all $g \in G$. Consequently, if $a \in F$, and $a\omega(g) = 0$ for all $g \in G$, then $a = 1$. We see that any set containing one character is independent.

Suppose that any set of fewer than n distinct characters of a group G in a field F are independent. Let $\omega_1, \ldots, \omega_n\colon G \to F^\times$ be distinct characters, and suppose we have elements $a_i \in F$ such that

$$a_1\omega_1(g) + \cdots + a_n\omega_n(g) = 0$$

for all $g \in G$.

We need to show that $a_i = 0$ for all i. Suppose otherwise. The nwe can find i such that $a_i \neq 0$. It follows that all of the coefficients a_i must be non-zero; otherwise, we have a set of less than n distinct but non-independent characters, which contradicts our inductive hypothesis.

Write $b_i = a_i/a_n$. Then

$$b_1\omega_1(g) + \cdots + b_{n-1}\omega_{n-1}(g) + \omega_n(g) = 0$$

for all $g \in G$.

Since $\omega_1 \neq \omega_n$, we can find $g_0 \in G$ such that $\omega_1(g_0) \neq \omega_n(g_0)$. Replacing g by $g_0 g$ and using that fact that the ω_i are isomorphisms, we see

$$b_1\omega_1(g_0)\omega_1(g) + \cdots + b_{n-1}\omega_{n-1}(g_0)\omega_{n-1}(g) + \omega_n(g_0)\omega_n(g) = 0$$

Multiplying by $\omega_n(g_0)$, we see

$$b_1\omega_n(g_0)\omega_1(g) + \cdots + b_{n-1}\omega_n(g_0)\omega_{n-1}(g) + \omega_n(g_0)\omega_n(g) = 0$$

Let $c_i = b_i(\omega_n(g_0) - \omega_i(g_0))$. Then $c_1 \neq 1$ by definition of g_0, and subtracting the above two equations, we see

$$c_1\omega_1(g) + \cdots + c_{n-1}\omega_{n-1}(g) = 0$$

Hence the $(n-1)$ distinct characters $\omega_1, \ldots, \omega_{n-1}$ are not independent, which is a contradiction. □

We can repeat the above definition of independence for isomorphisms of fields.

Definition 86 Let $\sigma_1, \ldots, \sigma_n\colon E \to E'$ be isomorphisms of fields. Then we call $\sigma_1, \ldots, \sigma_n$ *independent* if whenever there are elements $a_1, \ldots, a_n \in E'$ such that

$$a_1\sigma_1(a) + \cdots + a_n\sigma_n(a) = 0$$

for all $a \in E$, then $a_i = 0$ for all i.

Since a field isomorphism $\sigma\colon E \to E'$ restricts to a character of the group $E^\times$ in E', the above result has the following corollary.

Corollary 87 *Let $\sigma_1, \ldots, \sigma_n \colon E \to E'$ be distinct isomorphisms between two fields. Then the characters $\sigma_1, \ldots, \sigma_n$ are independent.* □

If we have an automorphism $\sigma \colon E \to E$ of a field E, a *fixed point* of E under σ is an element $a \in E$ such that $\sigma(a) = a$. The following definition generalises this concept.

Definition 88 Let $\sigma_1, \ldots, \sigma_n \colon E \to E'$ be isomorphisms of fields. We call an element $a \in E$ such that $\sigma_1(a) = \cdots = \sigma_n(a)$ a *fixed point* of E *under* $\sigma_1, \ldots, \sigma_n$.

The proof of the following straightforward result is left as an exercise.

Lemma 89 *The set of fixed points of a field E under a set of isomorphisms is a subfield of E.* □

We call the subfield of fixed points under a set of isomorphisms the *fixed field*.

Theorem 90 (Fixed Field Theorem) *Let $\sigma_1, \ldots, \sigma_n \colon E \to E'$ be distinct isomorphisms between fields. Let F be the fixed field of E under $\sigma_1, \ldots, \sigma_n$. Then* $\deg(E/F) \geq n$.

Proof: Suppose that $\dim(E/F) = r < n$. Let $\{e_1, \ldots, e_r\}$ be a basis of E, as a vector space over F.

The homogenous set of equations in x_i

$$\begin{array}{rcl} \sigma_1(e_1)x_1 + \cdots + \sigma_n(e_1)x_n & = & 0 \\ \sigma_1(e_2)x_1 + \cdots + \sigma_n(e_2)x_n & = & 0 \\ \vdots & & \vdots \\ \sigma_1(e_r)x_1 + \cdots + \sigma_n(e_r)x_n & = & 0 \end{array}$$

has a non-trivial solution since $r < n$.

Let $a \in E$. Then we can find $a_i \in F$ such that

$$a = a_1 e_1 + \cdots + a_r e_r$$

Since a_i is a fixed point, we can write

$$b_i = \sigma_1(a_i) = \cdots = \sigma_n(a_i)$$

Certainly

$$\begin{array}{rcl} b_1\sigma_1(e_1)x_1 + \cdots + b_1\sigma_n(e_1)x_n & = & 0 \\ b_2\sigma_1(e_2)x_1 + \cdots + b_n\sigma_n(e_2)x_n & = & 0 \\ \vdots & & \vdots \\ b_r\sigma_1(e_r)x_1 + \cdots + b_r\sigma_n(e_r)x_n & = & 0 \end{array}$$

so

$$\begin{array}{rcl} \sigma_1(a_1e_1)x_1 + \cdots + \sigma_n(a_1e_1)x_n & = & 0 \\ \sigma_1(a_2e_2)x_1 + \cdots + \sigma_n(a_2e_2)x_n & = & 0 \\ \vdots & & \vdots \\ \sigma_1(a_re_r)x_1 + \cdots + \sigma_n(a_re_r)x_n & = & 0 \end{array}$$

Now

$$\sigma_i(a_1e_1) + \cdots + \sigma_i(a_re_r) = \sigma_i(a)$$

so, adding the above equations

$$\sigma_1(a)x_1 + \cdots + \sigma_n(a)x_n = 0$$

It follows that the isomorphisms $\sigma_1, \ldots, \sigma_n$ are not independent, which is a contradiction of corollary 87. □

In particular, we have the following result, which is perhaps the most useful from the point of view of applications.

Corollary 91 *Let $\sigma_1, \ldots, \sigma_n \colon E \to E$ be distinct automorphisms of a field E. Let F be the fixed field of E under $\sigma_1, \ldots, \sigma_n$. Then* $\deg(E/F) \geq n$. □

We can also go slightly in the other direction with our definitions. We begin with the following obvious result.

Lemma 92 *Let E be an extension of a field F. Then the set of automorphisms of E which leave F fixed is a subgroup of the group of automorphisms of E.* □

We write $G(E, F)$ to denote the group of automorphisms of the field E which leave the field F fixed. We call $G(E, F)$ the *group of automorphisms of E relative to F*.

The following result is then a reformulation of the fixed field theorem.

Theorem 93 (Relative Automorphism Theorem) *Let E be a finite extension of a field F. Let $G(E, F)$ be the group of automorphisms of E relative to F. Then $G(E, F)$ is finite, and*

$$|G(E, F)| \leq \deg(E/F)$$

□

Exercises

1. Let σ be a character of a group G in some field F. Let $[G, G]$ be the commutator of G. Prove that σ factors through the quotient map $\pi \colon G \to G/[G, G]$.

2. Prove lemma 89.

3. Prove lemma 92

4. Use the fixed field theorem to deduce the relative automorphism theorem.

13 Symmetric Polynomials

Let K be a field. Let $E = K(x_1, \ldots, x_n)$ be the field of rational functions of the variables $x_1, \ldots, x_n$.

A permutation $\sigma \in \Sigma_n$ can be considered to be an automorphism $\sigma \colon E \to E$ by writing

$$\sigma(f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

Definition 94 A *symmetric function* on K is a fixed point of the field E under the group of automorphisms Σ_n.

Let F be the field of symmetric functions.

Definition 95 We define the *elementary symmetric functions*

$$\begin{array}{rcl} a_1(x_1, \ldots, x_n) & = & \sum_{i=1}^{n} x_i \\ a_2(x_1, \ldots, x_n) & = & \sum_{i<j} x_i x_j \\ a_3(x_1, \ldots, x_n) & = & \sum_{i<j<k} x_i x_j x_k \\ \vdots & & \vdots \\ a_n(x_1, \ldots, x_n) & = & x_1 \cdots x_n \end{array}$$

We have an extension, $S = K(a_1, \ldots, a_n)$, of the field K generated by the elementary symmetric functions. Since the functions a_i are symmetric functions, S is a subfield of F.

Theorem 96 *The fields S and F are equal, and* $\deg(E/F) = n!$.

Proof: The group Σ_n has n! elements. By the fixed field theorem, we know that $\deg(E/F) \geq n!$.

Since S is a subfield of F, it suffices to show that $\deg(E/S) \leq n!$. Consider the polynomial

$$p(t) = ()t - x_1)(t - x_2) \cdot (t - x_n)$$

Then

$$p(t) = t^n - a_1 t^{n-1} + a_2 t^{n-2} - \cdots + (-1)^n a_n$$

Thus $p(t)$ can be considered to be a polynomial over the field S, generated by the elementary symmetric functions. The polynomial $p(t)$ splits over the field $E = K(x_1, \ldots, x_n)$. Hence the splitting field of $p(t)$ is contained in the field E.

The splitting field for the polynomial $p(t)$ must contain the coefficent field, S, and so the field K, and all of the roots x_n. The smallest field with this property is E itself. Therefore E is the splitting field for the polynomial $p(t)$, so by proposition 51, it follows that $\deg(E/S) \leq n!$, and we are done. □

Exercises

1. Prove that the elementary symmetric functions are indeed symmetric functions.

2. Let K be a field. Let $E = K(x)$ be the field of all rational functions of one variable with coefficients in K. Prove that we have a group, G, of six automorphisms of E generated by the automorphisms

$$\sigma_1 \colon f(x) \mapsto f(\frac{1}{x}) \qquad \sigma_2 \colon f(x) \mapsto f(1-x)$$

3. Let F be the fixed field of the above group G. Let

$$i(x) = \frac{(x^2 - x + 1)^3}{x^2(x-1)^2}$$

Prove that $I(x) \in F$.

4. Let $S = K(I)$ be the field of all rational functions of I. Prove that $S = F$, and $\deg(E/F) = 6$.

14 Normal Extensions

Definition 97 Let E be an extension of a field F. Let $G(E, F)$ be the group of extensions of E relative to F. Then we call E a *normal extension* of F if $\deg(E/F) < \infty$, and the fixed field of the group $G(E, F)$ is precisely F.

IF E is a normal extension of a field F, $\deg(E/F)$ is finite. By the relative automorphism theorem, $|G(E, F)| \leq \deg(E/F)$. Hence the group $G(E, F)$ is finite,

Example 98 Let $\sigma \colon \mathbb{C} \to \mathbb{C}$ be an automorphism of the complex numbers that leaves the real numbers fixed. Then

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$$

so $\sigma(i) = \pm 1$, and $\sigma(z) = z$ or $\sigma(z) = \overline{z}$ for all $z \in \mathbb{C}$.

Thus, we see that the group $G(\mathbb{C}, \mathbb{R})$ has precisely two elements. An element of the field $\mathbb{C}$ is in the fixed field of $G(\mathbb{C}, \mathbb{R})$ precisely when $\sigma(z) = \overline{z}$, that is to say $z \in \mathbb{R}$.

Thus, $\mathbb{C}$ is a normal extension of the field $\mathbb{R}$.

Example 99 Let ω be a cube root of the number 2. Let $\sigma \colon \mathbb{Q}(\omega) \to \mathbb{Q}(\omega)$ be an automorphism that leaves the field $\mathbb{Q}$ fixed. Then

$$\sigma(\omega)^3 = \sigma(\omega^3) = \sigma(2) = 2$$

so $\sigma(\omega) = \omega$, since there is only one cubic root of 2 in the field $\mathbb{Q}(\omega)$.

It follows that ω is the identity element of the field $\mathbb{Q}(\omega)$. Hence the group $G(\mathbb{Q}(\omega), \mathbb{Q})$ contains only the identity map, and the fixed field of the group $G(\mathbb{Q}(\omega), \mathbb{Q})$ is the entire field $\mathbb{Q}(\omega)$.

Therefore, $\mathbb{Q}(\omega)$ is not a normal extension of the field $\mathbb{Q}$.

Theorem 100 *Let E be a normal extension of a field F, and let H be a subgroup of $G(E, F)$. Let E_H be the fiexed field of K. Then*

- $\deg(E/E_H) = |H|$.
- $H = G(E, E_H)$.

Proof: By the above remark, the group $G(E, F)$ is finite, so the subgroup H is also finite. Write

$$H = \{\sigma_1, \ldots, \sigma_n\}$$

write σ_1 is the identity automorphism.

By the fixed field theorem, we already know that $\deg(E/E_H) \geq n$. Suppose that $\deg(E/E_H) > n$. Then we can find aelements $\{e_1, \ldots, e_{n+1}\}$ of the field E_H which are linearly independent with respect to the field F.

There is a non-trivial solution in E to the set of equations

$$\begin{aligned} \sigma_1(e_1)x_1 + \cdots + \sigma_1(e_{n+1})x_{n+1} &= 0 \\ \vdots & \quad \vdots \\ \sigma_n(e_1)x_1 + \cdots + \sigma_n(e_{n+1})x_{n+1} &= 0 \end{aligned}$$

This solution cannot be in the field F, since the elements $e_1, \ldots, e_{n+1}$, are linearly independent over F, and the automorphism σ_1 is the identity.

Choose such a non-trivial solution so that as many of the elements $x_i \in E_H$ as possible are zero.[2] Changing the order of the automorphisms and elements e_i if necessary, we can assume that this solution takes the form

$$a_1, \ldots, a_r, 0, \ldots, 0 \qquad a_i =\neq 0$$

Observe that $r \neq 1$, since othersie $a_1\sigma_1(e_1) = 0$, so $\sigma_1(e_1) = e_1 = 0$, which contradicts linear independence of the set $\{e_1, \ldots, e_{n+1}\}$ over F. Multiplying by a_r^{-1}, we can assume that $a_r = 1$. Thus

$$a_1\sigma_i(e_1) + \cdots + a_{r-1}\sigma_i(e_{r-1}) + \sigma_i(e_r) = 0$$

for all i.

At least one of the above a_i cannot be in the field F. Say $a_1 \in E_H \backslash F$. Hence there is an automorphism σ_k such that $\sigma_k(a_1) \neq a_1$.

By the above equation

$$\sigma_k(a_1)\sigma_k\sigma_j(e_1) + \cdots + \sigma_k(a_{r-1})\sigma_k\sigma_j(e_{r-1}) + \sigma_k\sigma_j(e_r) = 0$$

Since $H = \{\sigma_1, \ldots, \sigma_n\}$ is a group, we can choose j and k such that $\sigma_k\sigma_j = \sigma_i$. Hence

$$\sigma_k(a_1)\sigma_i(e_1) + \cdots + \sigma_k(a_{r-1})\sigma_i(e_{r-1}) + \sigma_i(e_r) = 0$$

Subtracting from our original equation, we see that

$$(a_1 - \sigma_k(a_1)\sigma_i(e_1) + \cdots + (a_{r-1} - \sigma_k(a_{r-1})\sigma_i(e_{r-1}) = 0$$

for all i.

Since $a_1 \neq \sigma_k(a_1)$, we have a non-trivial solution the above system of equations having fewer than r non-zero elements. This contradicts our choice of r. If follows that our assumption that $\deg(E/E_H) > n$ is false, so $\deg(E/E_H) = n$.

[2]But of course, not all of the x_i can be zero otherwise we just have the trivial solution.

To prove the second statement, observe that $H \subseteq G(E, E_H)$, so $|H| \leq |G(E, E_H)|$. We know that $\deg(E/E_H) = |H|$, and by the relative automorphism theorem, $\deg(E/E_H) \geq |G(E, E_H)|$. It thus follows that $H = G(E, E_H)$. □

Corollary 101 *There are no two distinct finite groups of automorphisms of a given field with the same fixed field.* □

Definition 102 Let F be a field. Let E be an extension of F. Then we call an element $a \in E$ *separable* if it is the root of some separable polynomial over F.

We call an extension *separable* if every element is separable.

Lemma 103 *Let E be a normal extension of a field F. Then E is separable. Further, any element of E is a root of an irreducible separable polynomial over F which splits in E.*

Proof: Write $G(E, F) = \{\sigma_1, \ldots, \sigma_n\}$. Let $a \in E$, and let

$$\{a_1, \ldots, a_r\}$$

be the set of distinct elements of the set

$$\{\sigma_1(a), \ldots, \sigma_n(a)\}$$

where $a_1 = a$.

Since $G(E, F)$ is a group,

$$\sigma_j(a_i) = \sigma_j\sigma_i(a) = \sigma_k(a) = a_k$$

for some k.

The polynomial

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

,and so its coefficients, is fixed by the group $G(E, F)$. Since the extension E is normal, F is the fixed field of the group $G(E, F)$. Therefore $f(x) \in F[x]$. By construction, $f(a) = 0$, and $f(x)$ is separable. Therefore the extension E is separable.

Suppose that a is a root of a polynomial $g(x) \in F[x]$. Then each automorphism σ_i fixes the coefficients of the polynomial $g(x)$. Therefore

$$\sigma_i(g(a)) = g(\sigma_i(a)) = 0$$

so the polynomial $g(x)$ has r distinct roots, $a_1, \ldots, a_r$. Hence $\deg g(x) \geq r$, and it follows that the polynomial $f(x)$ is irreducible. □

Theorem 104 *Let F be a field. Then an extension ,E, of F is normal if and only if it is the splitting field of some polynomial over F.*

Proof: Suppose that E is the splitting field of a separable polynomial $p(x) \in F[x]$.

If all of the roots of $p(x)$ lie in F, then the result is trivial, since $E = F$ and only the identity automorphism of E then leaves F fixed,

Suppose $p(x)$ has $n > 1$ roots in E, but not in F. Working by induction, suppose that for all splitting fields, E', of a polynomial $f(x) \in F'[x]$ with fewer than n roots of $f(x)$ lying outside of F', the extension E' is normal.

Let

$$p(x) = p_1(x) \cdots p_r(x)$$

be a factorisation of $p(x)$ into irreducible factors. At least one of these factors, say $p_1(x)$, has degree greater than one; otherwise the polynomial $p(x)$ would split in the field F.

Let $a_1 \in E$ be a root of $p_1(x)$. Then by theorem 37

$$\deg(F(a_1)/F) = \deg(p_1(x)) = s$$

Since the polynomial $p(x)$ is separable, the irreducible factor $p_1(x)$ has distinct roots $a_1, \ldots, a_s \in E$. By corollary 38, there are isomorphisms $\sigma_i \colon F(a_1) \to F(a_i)$, such that $\sigma_i(a_1) = a_i$, each of which leave the field F fixed.

Now, the extension E is a splitting field for the polynomial $p(x)$ over the field $F(a_i)$. Hence, by theorem 53, the isomorphism σ_i can be extended to an automorphism $\tilde{\sigma_i} \colon E \to E$ that leaves F fixed, and has the property that $\tilde{\sigma_i}(a_1) = a_i$.

Observe that fewer than n roots of the polynomial $p(x)$ lie outside of $F(a_1)$. Hence, by inductive hypothesis, the field E is a normal extension of the field $F(a_1)$. In particular, any element in E which is not in $F(a_1)$ is changed by at least one automorphism of E which leaves $F(a_1)$ fixed.

Let $\theta \in E$ be fixed under all automorphisms of E that leave F fixed. Then $\theta \in F(a_1)$, so we can write

$$\theta = c_0 + c_1 a_1 + c_2 a_2^2 + \cdots + c_{s-1} a_1^{s-1}$$

where $c_i \in F$. Hence $\tilde{\sigma_i}(\theta) = \theta$, and

$$\theta = c_0 + c_1 a_i + c_2 a_i^2 + \cdots + c_{s-1} a_i^{s-1}$$

for all i.

The polynomial

$$c_{s-1} x^{s-1} + c_{s-2} x^{s-12} + \cdots + c_1 x + (c_0 - \theta)$$

has roots $a_1, \ldots, a_s$, that is to say more roots than its degree. Therefor it must be zero. In particular, $c_0 - \theta = 0$, and $\theta \in F$. It follows that E is a normal extension of F.

Fortunately, using the above lemma, the converse result is far more straightforward to prove. Let E be a normal extension of F. Let $\deg(E/F) = n$, and let $\{e_1, \ldots, e_n\}$ be a basis of E as a vector space over F. By the above lemma, we can find a separable polynomial $f_i(x) \in F[x]$ with e_i as a root.

The extension E is the splitting field of the polynomial

$$p(x) = f_1(x) \cdots f_n(x)$$

□

14.1 Exercises

1. Prove corollary 101.

2. Let E be a normal extension of a field F. Let E' be a normal extension of the field E. Prove that E' is a normal extension of F.

15 Roots of Unity

The following result follows from the theory we have already developed; the proof is left as an exercise.

Proposition 105 *Let F be a field of characteristic p. Let $n \in \mathbb{N}^{>0}$ not divide p. Then the polynomial $x^n - 1$ has n distinct roots in its splitting field.* □

In the above proposition, it is possible that $p = 0$. By the theorem 104, the splitting field of the polynomial $x^n - 1$ is a normal extension.

Proposition 106 *The roots of the polynomial $x^n - 1$ in the splitting field form a cyclic group with n elements under multiplication.*

Proof: Let S be the set of roots. Clearly $1 \in S$. Let $a \in S$, so that $a^n - 1 = 0$. Then

$$(a^{-1})^n - 1 = (a^{-1})^n(1 - a^n) = 0$$

so $a^{-1} \in S$.

Let $a, b \in S$. Then $a^{-1} \in S$, so

$$(a^{-1})^n - 1 = 0 \qquad b^n - 1 = 0$$

and

$$(ab)^n - 1 = a^n(b^n - (a^{-1})^n)$$

But

$$(a^{-1})^n = b^n = 1$$

so

$$(ab)^n - 1 = 0$$

and the set S is a group. By the above proposition, the set S has n elements. The set S is therefore a cyclic group by theorem 74. □

The elements of S thus take the form

$$1, a, a^2, \ldots, a^{n-1}$$

for some generator a.

Definition 107 A generator a of the group S is called a *primitive n-th root of unity.*

Proposition 108 *Let F be a field, and let E be the field obtained from F by adjunction of a primitive n-th root of unity. Then the group $G(E, F)$ is abelian, and is cyclic if n is a prime number.*

Proof: Let a be a primitive n-th root of unity. Then $E = F(a)$. Let $\sigma \in G(E, F)$. Then the image $\sigma(a)$ is also a root of the equation $x^n - 1$, so by the above, $\sigma(a) = a^{\alpha(\sigma)}$, where

$$\alpha(\sigma) \in \{1, 2, \ldots, n-1\}$$

We thus have a map $\alpha \colon G(E, F) \to \mathbb{Z}/n$, where $\mathbb{Z}/n$ denotes the set of integer numbers modulo n. Let $\sigma, \tau \in G(E, F)$ be distinct. Since $E = F(a)$, $\sigma(a) \neq \tau(a)$. Hence the map α is injective.

Let $\sigma(a) = a^k$ and $\tau(a) = a^l$. Then

$$\sigma\tau(a) = \sigma(a^k) = (\sigma(a))^k = (a^l)^k = a^{lk}$$

Thus α is an injective linear homomorphism from $G(E, F)$ into the multiplicative subgroup of the set $\mathbb{Z}/n$. Multiplication of integers modulo n is commutative, so the group $G(E, F)$ is commutative.

Let p be a prime number. Then the multiplicative group of the set $/Z/p$ is a cyclic group. Hence the group $G(E, F)$ is also cyclic. □

Exercises

1. Prove proposition 105
2. Show that the splitting field of the polynomial $x^n - 1$ is obtained by adjunction of a primitive n-th root of unity.

16 The Galois Group

Definition 109 Let F be a field, and let $p(x) \in F[x]$. Let E be the splitting field of $p(x)$. Then we call the group of relative automorphisms $G(E, F)$ the *Galois group* of $p(x)$.

By theorem 104, the splitting field E is a normal extension of the field F. Thus by theorem 100, the relative automorphism group $G(E, F)$ is finite.

Theorem 110 (The fundamental theorem of Galois theory) *Let $p(x)$ be a separable polynomial over a field F. Let E be the splitting field of $p(x)$, and let $G(E, F)$ be the Galois group. Then:*

- *Each intermediate field, B, of the extension E is the fixed field for some subgroup, G_B, of $G(E, F)$. The subgroup G_B is uniquely determined by the intermediate field B.*
- *An intermediate field, B, is a normal extension of the field F if and only if the subgroup G_B is a normal subgroup. If the field B is a normal extension, then the groups $G(B, F)$ and $G(E, F)/G_B$ are isomorphic.*
- *For each intermediate field, B,*

$$\deg(B/F) = |G(E, F)/G_B| \qquad \deg(E/B) = |G_B|$$

Proof: Let B be an intermediate field. Then E is the spliting field of the polynomial $p(x)$ when considered as a polynomial over the field B. By theorem 104, E is a normal extension of the field B. Hence B is the fixed field of some group of automorphisms of the field E. Any automorphism of the field E that fixes the field E also fixes the subfield F. Thus $G_B = G(E, B)$ is a subgroup of the Galois group $G(E, F)$.

By corollary 101, the subgroup G_B is uniquely determined by the intermediate field B, and we have the first part of the theorem.

By the above, the intermediate field B is the fixed field of the group G_B. According to theorem 100, it follows that $\deg(E/B) = |G_B|$. By proposition 6

$$\deg(E/F) = \deg(E/B)\deg(B/F)$$

By Lagrange's theorem for finite groups

$$|G(E, F)| = |G(E, F)/G_B||G_B|$$

By theorem 100, $\deg(E/F) = |G(E, F)|$. Hence

$$\deg(E/B) = |G_B|$$

and we have the third part of the theorem.

It remains to prove the second part of the theorem. We know that the number $|G(E, F)/G_B|$ is the number of left cosets of the subgroup G_B. Each element $\sigma \in G(E, F)$ induces an isomorphism $\sigma|_B \colon B \to B'$, where B' is some other subfield of E. The field B' is an extension of the field F, and the isomorphism σ fixes the field F. An element $\sigma \in G(E, F)$ belongs to the subgroup G_B if and only if the induced isomorphism $\sigma|_B$ is the identity isomorphism on the field B.

We claim that $\sigma_1|_B = \sigma_2|_B$ if and only if the isomorphisms σ_1 and σ_2 belong to the same coset. To see this, suppose

$$\sigma_1 G_B = \sigma_2 G_B$$

Then we can find $\sigma \in G_B$ such that $\sigma_1 = \sigma_2\sigma$, and by the above remark

$$\sigma_1|_B = \sigma_2|_B \circ 1_B = \sigma_2|_B$$

Conversely, suppose that $\sigma_1|_B = \sigma_2|_B$. Then $\sigma_1(a) = \sigma_2(a)$ for all $a \in B$, so $\sigma_1^{-1} \circ \sigma_2(a) = a$ for all $a \in B$. Hence, $\sigma_1^{-1}|_B \circ \sigma_2|_B = 1_B$, and by the above remark, $\sigma_1^{-1} \circ \sigma_2 \in G_B$. It follows that the elements σ_1 and σ_2 belong to the same coset, which establishes our claim.

Let $\sigma \colon B \to B'$ be an isomorphism that fixes the field F, where B' is a subfield of E. Then σ maps the polynomial $p(x)$ to itself, and so can be extended to an isomorphism $\tilde{\sigma} \colon E \to E$ of the splitting field. Certainly, $\tilde{\sigma}|_B = \sigma$.

Hence the isomorphisms $\sigma \colon B \to B'$ of the above form correspond to the set of cosets $G(E, F)/G_B$. The relative automorphism group, $G_{B'}$, of the field B', is the subgroup $\sigma G_B \sigma^{-1}$.

Suppose that B is a normal extension of the field F. By theorem 100, $|G(B, F)| = \deg(B/F)$. Conversely, suppose that $|G(B, F)| = \deg(B/F)$.

Let F' be the fixed field of the group $G(B, F)$. Then $F < F' < B$, and by construction B is a normal extension of the field F'. Thus, by theorem

100, $\deg(B/F') = |G(B,F)| = \deg(B/F)$. Hence $F = F'$, and B is a normal extension of the field F.

We have thus shown that the intermediate field B is a normal extension of the field F if and only if $|G(B,F)| = \deg(B/F)$.

By the third part of the theorem, which we have already proved, we know that $\deg(B/F) = |G(E,F)/G_B|$. We saw above that the isomorphisms $\sigma\colon B \to B'$ into E that leave F fixed correspond to the set of cosets $G(E,F)/G_B$. Applying once more the third part of the theorem, there are $|\deg(B/F)|$ such cosets.

Thus the intermediate field B is a normal extension if and only if there are $|G(B,F)|$ isomorphisms $\sigma\colon B \to B'$ into E that leave F fixed. Then elements of the group $G(B,F)$ are automorphisms $\sigma\colon B \to B$ that leave F fixed. Therefore B is normal if and only if $\sigma B = B$ whenever $\sigma\colon B \to B'$ is an isomorphism into E that leaves F fixed.

Let $\sigma\colon E \to E$ be an element of the group $G(E,F)$. Rephrasing the above conclusion, the extension B is normal if and only if $\sigma B = B$. But $\sigma B = B$ if and only if $\sigma G_B \sigma^{-1} \in G_B$. Thus the extension B is normal if and only if the subgroup G_B is normal.

The last sentence of the second part of the theorem follows from the above analysis; the precise details are left as an exercise. □

In the above theorem, note that $G_B = G(E,B)$. Thus G_B is the Galois group of the polynomial $p(x)$ when considered as a polynomial over the field B.

Exercises

1. Let E and B be normal extensions of a field F such that B is a subfield of E. Show that the groups $G(B,F)$ and $G(E,F)/G_B$ are isomorphic.

17 Simple Extensions

Before looking at applications of Galois theory in the outside world, we will examine another concept in the theory of field extensions.

Definition 111 Let E be an extension of a field F. We call E a *simple extension* if $E = F(a)$ for some element $a \in E$.

Theorem 112 *Let E be a finite extension of a field F. Then E is simple if and only if there are a finite number of intermediate number of intermediate fields.*

Proof: Let $E = F(a)$, where $a \in E$. Let $f(x) \in F[x]$ be an irreducible equation with a as a root. Then the polynomial $f(x)$ is the polynomial of the lowest possible degree such that this property holds. Let B be an intermediate field, and let $g(x)$ be an irreducible polynomial over B such that $g(a) = 0$.

Define an intermediate field B' by adjoining the coefficients of the polynomial $g(x)$ to the field F. Then $g(x)$ is an irreducible polynomial over B'. Since $E = B'[a]$, by theorem 37, $\deg(E/B) = \deg(E/B')$. Hence $B = B'$.

Thus the intermediate field B is uniquely determined by the polynomial $g(x)$. But the polynomial $g(x)$ is a factor of the polynomial $f(x)$, and, up to multiplication by a consstant, there are only finitely many factors of the

polynomial $f(x)$ in the field E. It follows that there are only finitely many intermediate fields.

Conversely, suppose the extension E has only finitely many intermediate fields. Suppose that the field F is finite. Since $\deg(E/F) < \infty$, the field E is also finite. Hence, by theorem 74, the set of non-zero elements of the field E is a cyclic group under the operation of multiplication. Choose a generator, $a \in E$, of this group. Then $E = F(a)$, and we are done.

We can therefore assume that the field F is infinite. Let $a, b \in E$. Then we claim that there is an element $c \in E$ such that $F(a, b) = F(c)$.

Write

$$c_\alpha = a + \alpha b$$

where $\alpha \in F$. Since there are infinitely many elements α, and only finitely many intermediate fields, we can find elements $\alpha_1, \alpha_2 \in F$ such that $\alpha_1 \neq \alpha_2$ and $F(c_{\alpha_1}) = F(c_{\alpha_2})$.

Certainly, $c_{\alpha_1}, c_{\alpha_2} \in F(c_{\alpha_1})$. Therefore

$$c_{\alpha_1} - c_{\alpha_2} = (\alpha_1 - \alpha_2)b \in F(c_{\alpha_1})$$

so $b \in F(c_{\alpha_1})$, and $a = c_{\alpha_1} - \alpha_1 b \in F(c_{\alpha_1})$. Thus $F(a, b) \subseteq F(c_{\alpha_1})$. But certainly $F(c_{\alpha_1}) \subseteq F(a, b)$, so we have proved our claim.

Choose an element $c \in F(a, b)$ so that $\deg(F(c)/F)$ is as large as possible. Let $d \in E$. Then, by the above, we can find an element $c' \in E$ such that $F(c, d) = F(c')$. It follows that $\deg(F(c')/F) = \deg(F(c, d)/F) \geq \deg(F(c)/F)$.

Since we chose the degree $\deg(F(c)/F)$ to be as large as possible, we see that $\deg(F(c, d)/F) = \deg(F(c)/F)$. Hence $F(c, d) = F(c)$. Thus $d \in F(c)$, which means that $E = F(c)$, and we are done. □

Corollary 113 *Let F be a field, let $a_1, \ldots, a_n \in E$, and let $E = F(a_1, \ldots, a_n)$, where $a_1, \ldots, a_n$ are separable elements of the field E. Then we can find an element $b \in E$ such that $E = F(b)$.*

Proof: Let $f_i(x)$ be an irreducible equation over the field F such that $f_i(a_i) = 0$. Then E is the splitting field of the product $f_1(x) \cdots f_n(x)$, and let $G(E, F)$ be the Galois group.

Let B be an intermediate field. Then by the fundamental theorem of Galois theory, B is the fixed field of some subgroup, G_B, of the group $G(E, F)$. Since the Galois group is always finite, it follos that there are only finitely many intermediate fields. Thus, by the above theorem, the extension E is separable, and we are done. □

Corollary 114 *Let F be a field of characteristic zero. Let E be a finite extension of the field F. Then E is simple.*

Proof: Since the extension E is finite, we can write $E = F(a_1, \ldots, a_n)$, where $a_1, \ldots, a_n$ are algebraic elements of the field E. Let $f_i(x)$ be an irreducible equation over the field F such that $f_i(a_i) = 0$. Since the field F has characteristic zero, each polynomial $f_i(x)$ is separable by corollary 80. Consequently, each element a_i is separable, and we are done by the above corollary. □

Exercises

1. Let E be a finite separable extension of a field. Prove that E is simple.
2. Let E be an extension of a field F. Let $a, b \in F$ be separable elements. Prove that $F(a, b)$ is a separable extension of F.

18 Kummer Fields

The results we develop in this section will be improtant in our main application of Galois theory, where we look at solvability of polynomials in the next few sections.

Proposition 115 *Let F be a field of characteristic p. Suppose that F contains a primitive n-th root of unity. Then n is not divisible by p.*

Proof: Suppose $n = pq$. Then

$$y^p - 1 = (y - 1)^p$$

since p is a factor of ever coefficient except for the first and the last in the expansion of $(y - 1)^p$.

Thus

$$x^n - 1 = (x^q)^p - 1 = (x^q - 1)^p$$

and the polynomial $x^n - 1$ has at most q distinct roots.

Since the field F contains a primitice n-th root of unity, ϵ, we see that $1, \epsilon, \ldots, \epsilon^{n-1}$ are distinct roots of the polynomial $x^n - 1$. This last statement is a contradiction. Thus the number n is not divisible by p. □

Definition 116 Let F be a field that contains a primitive n-th root of unity. Then a *Kummer field* is a splitting field of a polynomial of the form

$$(x^n - a_1) \cdots (x^n - a_r)$$

where $a_i \in F$.

Theorem 117 *Let F be a field that contains a primitive n-th root of unity. Let E be a Kummer field over F. Then the following hold.*

- *The field E is a normal extension of F.*
- *The relative automorphism group, $G(E, F)$, is abelian.*
- *The lowest common multiple of the orders of the elements of the group $G(E, F)$ divides n.*

Proof: The field E is the splitting field of some polynomial

$$(x^n - a_1) \cdots (x^n - a_r)$$

where $a_i \in F$. Let $f(x) = x^n - a_i$, where $a_i \neq 0$. Then $f'(x) = nx^{n-1}$. Thus the derivative $f'(x)$ and polynomial $f(x)$ have no roots in common, and hence no common factors. By theorem 79, the polynomial $f(x)$ has no repeated roots.

It follows that the splitting field E is separable, and therefore, by theorem 104, normal.

To prove the second part, let b_i be a root of the polynomial $x^{n_i} - a_i$. Since the field F contains a primitive n-th root of unity, ϵ, we see that $b_i, b_i\epsilon, \ldots, b_i\epsilon^{n-1}$ are n distinct roots of the polynomial $x^n - a_i$. Therefore

$$E = F(b_1, \ldots, b_n)$$

Let $\sigma, \tau \in G(E, F)$. Then $\sigma(a_i) = \tau(a_i) = a_i$ since $a_i \in F$. It follows that σ and τ map roots of the polynomial $x^n - a_i$ to other such roots. We can therefore write

$$\sigma(b_i) = \varepsilon^{i_\sigma} b_i \qquad \tau(b_i) = \epsilon^{i_\tau} b_i$$

where $\epsilon \in F$.

Hence

$$\sigma\tau(b_i) = \sigma(\epsilon^{i_\tau} b_i) = \epsilon^{i_\sigma}\epsilon^{i_\tau} b_i = \tau\sigma(b_i)$$

But the elements b_i are generators of the field E with respect to the field F. Hence the relative automorphisms σ and τ commute. We conclude that the group $G(E, F)$ is commutative.

Now, for any element $\sigma \in G(E, F)$, we know that $\sigma(b_i) = \epsilon^{i_\sigma} b_i$, and $\sigma^k(b_i) = \epsilon^{i_\sigma k} b_i$. Since ϵ is a primitive n-th root of unity, $\varepsilon^{i_\sigma n} = 1$ for all i. Hence $\sigma^n(b_i) = 1$ for all n.

But the elements b_i are generators of the field E with respect to the field F. Hence $\sigma^n = 1$, and the order of σ divides n. This statement holds for all $\sigma \in G(E, F)$. Therefore the lowest common multiple of the orders of the elements of the group $G(E, F)$ divides n, and we are done. □

Corollary 118 *Let F be a field, and let p be a prime number. Suppose that F contains a primitive p-th root of unity. Let $a \in F$, and let E be the splitting field of the polynomial $x^p - a$. Then either $E = F$ and the polynomial $x^p - a$ is split in F, or $x^p - a$ is irreducible in F, and the group $G(E, F)$ is cyclic, of order p.* □

The above theorem has a converse. We first need a little terminology and two lemmas.

Definition 119 Let F be a field that contains a primitive n-th root of unity. Let G be a group. A homomorphism from the group G into the multiplicative group of n-th roots of unity in the field F is called a *character* of G.

The set of characters of any group is an abelian group. If a field F contains a primitive n-th root of unity, ϵ, it also contains a primitive m-th root of unity, $\epsilon^{n/m}$, whenever m divides n.

Lemma 120 *Let F be a field that contains a primitive n-th root of unity. Let E be a normal extension of F such that the relative automorphism group, $G(E, F)$,*

is abelian, and the lowest common multiple of the orders of the elements of the group $G(E,F)$ is equal to n.

Then the group $G(E,F)$ is isomorphic to its set of characters,

Proof: Since E is a normal extension of F, the group $G(E,F)$ is finite. Since it is abelian, we can write $G(E,F)$ is a product of cyclic groups

$$G(E,F) = G_1 \times \cdots \times G_r$$

where the group g_i has order m_i. By hypothesis, the number n is the lowest common multiple of the numbers m_i.

Let σ_i be the generator of the group G_i. Then there is a character, C_i, sending σ_i to ϵ_i, where ϵ_i is a primitive m_i-th root of unity, and σ_j to 1 when $j \neq i$.

Let Λ be the group of characters of the group $G(E,F)$. Then we have an isomorphism $\mathbb{C}\colon G(E,F) \to \Lambda$ defined by the formula

$$C(\sigma_1^{k_1} \cdots \sigma_r^{k_r}) = C_1^{k_1} \cdots C_r^{k_r}$$

□

The following result is left as an exercise.

Lemma 121 *Let E be a normal extension of the field F. Let n be the lowrst common multiple of the orders of elements of the group $G(E,F)$. Let $C\colon G(E,F) \to F^\times$ be a homomorphism.*

Then there is an element $a \in F$ such that $C(\sigma) = a/\sigma(a)$ for all $a \in G(E,F)$, and $a^n \in F$. □

Theorem 122 *Let F be a field that contains a primitive n-th root of unity. Let E be a normal extension of F such that the relative automorphism group, $G(E,F)$, is abelian, and the lowest common multiple of the orders of the elements of the group $G(E,F)$ divides n.*

Then E is a Kummer extension of the field F.

Proof: Let $b \in F\backslash\{0\}$. Suppose we have an element $a \in E$ such that $a^n = b$. Let ϵ be a primitive n-th root of unity in the field F. Then the polynomial $x^n - b$ has distinct roots

$$a, \epsilon a, \ldots, \epsilon^{n-1} a$$

and therefore splits in the field B.

Define A to be the set of all non-zero elements $a \in E$ such that $a^n \in F$. Then A is a multiplicative group, and the group $F^\times$ of all non-zero elements of the field F is a subgroup of A.

Let $F^\times, a_1 F^\times, \ldots a_r F^\times$ be the cosets of the subgroup $F^\times$ in A. Let $b_i = a_i^n \in F$. Then by the above, the field E splits the polynomial

$$f(x) = (x^n - a_1) \cdots (x^n - a_r)$$

We claim that E is the splitting field of the polynomial $f(x)$, which completes the proof. It suffices to show that $E = F(a_1, \ldots, a_r)$. We already know that $E \supseteq F(a_1, \ldots, a_r)$.

Suppose $E \neq F(a_1, \ldots, a_r)$. Then $F(a_1, \ldots, a_r)$ is an intermediate field between F and E. Since E is a normal extension of F, we can find a non-trivial automorphism, $\sigma \in G(E, F)$ which leaves $F(a_1, \ldots, a_r)$ fixed.

By lemma 120, we can find a character, $C(\sigma)$, of the group $G(E, F)$ such that $C(\sigma) \neq 1$. By lemma 121, we can write $C(\sigma) = a/\sigma(a)$, where $a \in E$ and $a^n \in F$.

By definition, $a \in A$, so we can write $a = a_i x$, where $x \in F^\times$. It follows that $a \in F(a_1, \ldots, a_r)$. By construction of the automorphism, σ, $\sigma(a) = a$, so $C(\sigma) = a/\sigma(a) = 1$, which is a contradiction.

Thus $E = F(a_1, \ldots, a_r)$, and we are done. □

Exercises

1. Prove corollary 118.
2. Prove lemma 121.
3. Prove that the map ϕ in the proof of lemma 120 is a well-defined isomorphism.

19 Solvable Groups

In this section we introduce a definition from group theory that will be useful to us when we use Galois theory to examine finding the roots of polynomials. We begin with some elementary results.

Proposition 123 *Let G be a group. Let G_1 and G_2 be subgroups of G, and let H_1 and H_2 be normal subgroups of G_1 and G_2 respectively. Then the following groups are isomorphic:*

$$\frac{H_1(G_1 \cap G_2)}{H_1(G_1 \cap H_2)} \qquad \frac{H_2(G_1 \cap G_2)}{H_2(H_1 \cap G_2)} \qquad \frac{G_1 \cap G_2}{(H_1 \cap G_2)(H_2 \cap G_1)}$$

□

Corollary 124 *Let G be a group, let H be asubgroup of G, and let N be a normal subgroup of G. Then the groups*

$$\frac{H}{H \cap N} \qquad \frac{HN}{N}$$

are isomorphic. □

Corollary 125 *Let G be a group, let H be asubgroup of G, and let N be a normal subgroup of G. Suppose that the quotient group G/N is abelian. Then the quotient group $H/H \cap N$ is also abelian.*

Proof: By the above corollary, the quotients $H/H \cap N$ and NH/N are isomorphic. The group NH/N is a subgroup of the abelian group G/N, and so is itself abelian. The result now follows. □

Definition 126 A group G is called *solvable* if we have a finite sequence of subgroups

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_s = \{1\}$$

where each entry G_i is a normal subgroup of the group G_{i-1}, and the quotient G_{i-1}/G_i is abelian.

To give a trivial example, any abelian group is solvable.

Proposition 127 *Any subgroup of a solvable group is solvable.*

Proof: Let G be a solvable group. Let H be a subgroup of G. Write

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_s = \{1\}$$

where each entry G_i is a normal subgroup of the group G_{i-1}, and the quotient G_{i-1}/G_i is abelian.

Define $H_i = H \cap G_i$, so that

$$H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_s = \{1\}$$

Each entry H_i is a normal subgroup of the group H_{i-1}, and the quotient H_{i-1}/H_i is abelian by corollary 125. □

Proposition 128 *The image of a solvable group under a homomorphism is solvable.* □

Corollary 129 *The quotient of a solvable group by a normal subgroup is solvable.* □

It turns out that large permuation groups are not solvable. Before we prove this, let us introduce some standard notation.

Definition 130 We define the symmetric group, Σ_n, to be the group of bijections of the set $\{1, 2, \ldots, n\}$. Elements of the group Σ_n are also called *permutations*. Given distinct numbers $a_1, \ldots, a_k \in \{1, 2, \ldots, n\}$, we define the *k-cycle*

$$(a_1\ a_2\ \cdots\ a_k)$$

to be the permuation sending a_i to a_{i+1} when $1 \leq i \leq k-1$, sending a_k to a_1, and leaving the other elements of the set $\{1, \ldots, n\}$ fixed.

Lemma 131 *Let $n > 4$. Let $G \subseteq \Sigma_n$ be a subgroup that contains every 3-cycle. Let $H \subseteq G$ be a normal subgroup such that G/H is abelian. Then the group H contains every 3-cycle.*

Proof: Let $\pi\colon G \to G/H$ be the quotient map. Let $i, j, k, r, s \in \{1, \ldots, n\}$ be distinct; this choice is possible since $n \geq 5$. Define

$$x = (i\ j\ k) \qquad y = (k\ r\ s)$$

Since the quotient G/H is abelian,

$$\pi(xyx^{-1}y^{-1} = \pi(x)\pi(y)\pi(x)^{-1}\pi(y)^{-1} = \pi(1)$$

so

$$xyx^{-1}y^{-1} \in H$$

But

$$xyx^{-1}y^{-1} = (i\ j\ k)(k\ r\ s)(k\ j\ i)(s\ r\ k) = (j\ k\ s)$$

We conclude that $(j\ k\ s) \in H$ for all distinct j, k, and s, and we are done. □

Theorem 132 *The group Σ_n is not solvable when $n > 4$.*

Proof: Suppose we have a sequence

$$\Sigma_n = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_s = \{1\}$$

where each entry G_i is a normal subgroup of the group G_{i-1}, and the quotient G_{i-1}/G_i is abelian.

The group $G_0 = G$ contains all 3-cycles. By the above lemma, the subgroup G_1 also contains all 3-cycles. Repeating this process, the subgroups $G_2, \ldots, G_s$ also contain all 3-cycles. Thus it cannot be true that $G_s = \{1\}$.

Hence the group Σ_n is not solvable.

□

Exercises

1. Prove proposition 123.
2. Prove corollary 124.
3. Give a non-abelian example of a solvable group.
4. Prove proposition 128.

20 Solvability by Radicals

Let $f(x)$ be a polynomial over a field F. We say that $f(x)$ is *solvable by radicals* if its roots can be found by a formula involving only the elements of the field F, and solutions of the equation $x^n - b = 0$ where $b \in F$.

More formally, we have the following.

Definition 133 Let F be a field. An extension, E, of the field F is called an *extension by radicals* if we can find intermediate fields $F = B_0, B_1, \ldots, B_r = E$ such that $B_i = B_{i-1}(a_i)$, where a_i is a solution of the equation $x^{n_i} - b_i = 0$ for some $b_i \in B_{i-1}$.

A polynomial $f(x) \in F[x]$ is said to be *solvable by radicals* if its splitting field lies within an extension by radicals.

Example 134 Let F be a field, and let ϵ be a primitive n-th root of unity in some extension of F. Then $F(\epsilon)$ is an extension of F by radicals.

The polynomial $x^n - 1$ splits over the field $F(\epsilon)$. Therefore, the polynomial $x^n - 1$ is always solvable by radicals.

Proposition 135 *Any extension of the field F by radicals can be extended to a normal extension by radicals.*

Proof: Let E be an extension of F by radicals. The we have intermediate fields $F = B_0, B_1, \ldots, B_r = E$ such that $B_i = B_{i-1}(a_i)$, where a_i is a solution of the equation $x^{n_i} - b_i = 0$ for some $b_i \in B_{i-1}$.

Let $B'_0 = F$. Define B'_i inductively to be the splitting field of the polynomial $x^{n_i} - b_i$ over the field B'_{i-1}. Then by theorem 104, the field B'_r is a normal extension of the field F that contains the extension E. □

Theorem 136 *A polynomial $f(x) \in F[x]$ is solvable by radicals if and only if its Galois group is solvable.*

Proof: Suppose that the polynomial $f(x)$ is solvable by radicals. Let E be a normal extension of the field F by radicals that contains the splitting field, B, of the polynomial $f(x)$. The we have intermediate fields $F = B_0, B_1, \ldots, B_r = E$ such that $B_i = B_{i-1}(a_i)$, where a_i is a solution of the equation $x^{n_i} - b_i = 0$ for some $b_i \in B_{i-1}$.

Let F' be the field attained from F by adjoining the n_i-th roots of unity for all i. Let B'_i be the corresponding extension of the field B_i. Then B'_i is a Kummer extension of the field B'_{i-1}, so the group $G(B'_i, B'_{i-1})$ is abelian by theorem 117.

We therefore have a sequence of groups

$$G(B'_r, B'_0) \supseteq G(B'_r, B'_1) \supseteq \cdots \supseteq G(B'_r, B'_r) = \{1\}$$

By the fundamental theorem of Galois theory, the subgroup $G(B'_r, B'_i)$ is a normal subgroup of the group $G(B'_r, B'_{i-1})$ for all i, and the quotient $G(B'_r, B'_{i-1})/G(B'_r, B'_i)$ is isomorphic to the group $G(B'_i, B'_{i-1})$, which is abelian as we remarked above.

Hence, by definition, the group $G(B'_r, B'_0)$ is solvable. Now, again applying the fundamental theorem of Galois theory, we have a normal subgroup

$$G(B'_r, B'_0) \subseteq G(B'_r, B_0)$$

and the quotient $G(B'_r, B_0)/G(B'_r, B'_0)$ is isomorphic to the group $G(B'_0, B_0)$, which is abelian by theorem 117. It follows that the group $G(B'_r, B_0)$ is solvable.

By corollary 129, the group $G(B, F) \cong G(B'_r, B_0)/G(B'_r, B_r)$ is thus solvable, and we have shown that a polynomial solvable by radicals has a solvable group.

Conversely, let B be the splitting field of the polynomial F, and suppose that the Galois group $G(B, F)$ is solvable. Let n be the order of the group $G(E, F)$, and let F' and B' be the fields attained by a primitive n-th root of unity to the fields F and B respectively. Then the group $G(B', F')$ is isomorphic to a subgroup of the group $G(B, F)$, and is therefore solvable.

Write

$$G(B', F') == G_0 \supseteq G_1 \supseteq \cdots \supseteq G_s = \{1\}$$

where each entry G_i is a normal subgroup of the group G_{i-1}, and the quotient G_{i-1}/G_i is abelian. Then by the fundamental theorem of Galois theory, there are intermediate normal extensions B'_i such that $G_i = G(B', B'_i)$. The quotient

$G(B', B'_{i-1})/G(B', B'_i)$ is isomorphic to the group $G(B'_i, B'_{i-1})$, and is therefore abelian.

By theorem 122, the field B'_i is a Kummer extension of the field B'_{i-1}. It follows that the field B' is an extension of the field F' by radicals. By construction, the field F' is an extension of the field F by radicals. Thus our original polynomial $f(x)$ is solvable by radicals, and we are done. □

Exercises

1. Prove that the extension B'_r constructed in the proof of proposition 135 is an extension by radicals.

2. Let B be the splitting field of a polynomial $f(x) \in F[x]$. Let n be the order of the group $G(E, F)$, and let F' and E' be the fields attained by a primitive n-th root of unity to the fields F and E respectively. Prove that the group $G(E', F')$ is isomorphic to a subgroup of the group $G(E, F)$.

3. In the above proof, show that the extension B'_i of the the field B'_{i-1} satisfies all the hypotheses of theorem 122.

21 Galois Groups over the Rationals

The following proposition is largely implicit in our earlier work, but is worth stating explicitly.

Proposition 137 *Let $f(x)$ be a polynomial of degree n. Then the Galois group of $f(x)$ is a subgroup of the symmetric group Σ_k, where $k \leq n$.*

Proof: Let $f(x) \in F[x]$. Let E be the splitting field of the polynomial $p(x)$. Then an automorphism, $\sigma \in G(E, F)$, that leaves F fixed leaves the coefficients of the polynomial $f(x)$ fixed, and so maps one root of the polynomial $p(x)$ to another root. Since σ is an automorphism, it is invertible as a map from E to E, and its inverse is also an automorphism.

Let $S = \{a_1, \ldots a_k\}$ be the set of distinct roots of the polynomial $p(x)$. Then certainly $k \leq n$, and we have a homomorphism $G(E, F) \to \Sigma_k$ defined by writing $\sigma \mapsto \sigma|_S$.

Since E is the splitting field of the polynomial $f(x)$, we can write $E = F(a_1, \ldots, a_k)$, so that the above homomorphism is injective. This statement completes the proof. □

Thus, if $f(x)$ is a polynomial of degree n, and the splitting field of $f(x)$ has degree $n!$, then by theorem 100, the Galois group of $f(x)$ has precisely $n!$ elements. In this case, it follows by the above proposition that the Galois group of $f(x)$ is isomorphic to the group Σ_n.

By theorem 132, in this case the Galois group of $f(x)$ is not solvable. By theorem 136, the polynomial $f(x)$ cannot be solved by radicals.

In order to apply the work of the previous section, we need Sylow's theorem, from group theory, which we state without proof.

Theorem 138 (Sylow's theorem) *Let G be a finite group, of order n. Let p be a prime number such that p^k is a factor of n, and $p^{k+1} \neq n$. Then G has a subgroup with p^k elements.*

Further, if G is a finite group with p^2 or p elements, then G has a subgroup with p elements. □

Theorem 139 *Let p be a prime number. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible equation of degree p. Suppose that $f(x)$ has exactly two non-real complex roots. Then the Galois group of $f(x)$ is isomorphic to Σ_p.*

Proof: Let E be the splitting field of the polynomial $f(x)$. Let a be a root of the polynomial $p(x)$. By theorem 37, $\deg(\mathbb{Q}(a), \mathbb{Q}) = p$. Certainly, $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq E$. Hence, by proposition 6, p is a factor of the number $\deg(E, F)$, so by theorem 100, p is a factor of the number $|G(E, F)|$. Therefore, by Sylow's theorem, the group $G(E, F)$ has a subgroup with p elements. In particular, $G(E, F)$ has an element of order p.

Let $a, \overline{a}, a_3, \ldots, a_p$ be the roots of the polynomial $f(x)$, where a and $\overline{a}$ are the complex roots. Then $a_i = \overline{a_i}$ when $i \geq 3$. By the fundamental theorem of algebra, the roots of the polynomial $f(x)$ can all be considered to lie in the field $\mathbb{C}$. We can therefore define an automorphism $\tau \in G(E, F)$ by the formula $\tau(z) = \overline{z}$.

Thus, $G(E, F)$ is isomorphic to a subgroup of the permutation group Σ_p, and contains a transposition, τ, and an element σ of order p. The only elements of order p in Σ_p are the p-cycles. But the group Σ_p is generated by a transposition and a p-cycle, so we are done. □

Example 140 Let $f(x) = 2x^5 - 10x + 5$. Then 5 is a factor of 5 and 10, but not of 2, and 5^2 is not a factor of 5. Therefore, by the Eisenstein criterion, the polynomial $f(x)$ is irreducible.

Observe that

$$f'(x) = 10x^4 - 10 = 10(x^2 + 1)(x + 1)(x - 1)$$

and

$$f''(x) = 40x^3$$

so $f''(x) > 0$ when $x > 0$ and $f''(x) < 0$ when $x < 0$.

Therefore the differentiable function $f(x)$ has a maximum when $x = -1$, and a minimum when $x = 1$. Further,

$$\lim_{x \to \pm\infty} f(x) = \pm\infty$$

Thus, looking at the graph of $f(x)$, we see that there are precisely 3 real numbers, a, where $f(a) = 0$. Thus $f(x)$ has precisely two complex roots.

By the above theorem, the polynomial $f(x)$ has Galois group isomorphic to Σ_5, and therefore cannot be solved by radicals over $\mathbb{Q}$.

Exercises

1. Let $f(x)$ be a real polynomial with exactly two complex roots. Prove that these roots are complex conjugates of each-other.

2. Prove that the group Σ_n is generated by the elements $(1\ 2)$ and $(1\ 2\ \cdots\ n)$.

3. Construct a degree 7 polynomial with Galois group Σ_7.