NOTES ON ALGEBRA (FIELDS)

Marc Culler - Spring 2005

The most familiar examples of fields are $\mathbb{F}_p \doteq \mathbb{Z}/p\mathbb{Z}$, where p is a prime, the field $\mathbb{Q}$ of rational numbers, the field $\mathbb{R}$ of real numbers and the field $\mathbb{C}$ of complex numbers. Another example to keep in mind is the field $F(t)$ of rational functions with coefficients in some field F.

1. The characteristic of a field

Definition 1.1. The *characteristic* of a commutative ring is either the smallest positive integer n such that $n \cdot 1 = 0$, or 0 if no such integer exists. The characteristic of a commutative ring R is denoted $\operatorname{Char} R$.

Exercise 1.1. Let F be a field of characteristic p. Show that $p \cdot x = 0$ for all $x \in F$.

Exercise 1.2. Show that if the characteristic of a field is not 0 then it is prime.

Exercise 1.3. Show that a finite field has non-zero characteristic.

Exercise 1.4. Let F be a field. Show that the intersection of any family of subfields of F is a subfield of F.

Proposition 1.2. *Let F be any field. The intersection of all subfields of F is a subfield which is isomorphic to $\mathbb{Q}$ if $\operatorname{Char} f = 0$, and isomorphic to $\mathbb{F}_p$ if $\operatorname{Char} F = p$.*

Proof. The intersection P of all subfields of F is a field by Exercise 1.4. Consider the ring homomorphism $\phi : \mathbb{Z} \to F$ given by $\phi(n) = n \cdot 1$. Since any subfield contains 1 and is closed under addition, $\operatorname{im} \phi$ is contained in P. If $\operatorname{Char} F = p \neq 0$ then $\operatorname{im} \phi$ is isomorphic to $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Since this is a field, we have $P = \operatorname{im} \phi \cong \mathbb{F}_p$. If $\operatorname{Char} F = 0$ then ϕ is injective. Define $\hat{\phi} : \mathbb{Q} \to F$ by $\hat{\phi}(m/n) = \phi(m)/\phi(n)$ for any $m, n \in \mathbb{Z}$ with $n \neq 0$. It is easy to check that $\hat{\phi}$ is well-defined, and is an injective homomorphism. Moreover, $\hat{\phi}(\mathbb{Q}) \subseteq P$ since P is closed under the field operations. Thus $P = \operatorname{im} \hat{\phi} \cong \mathbb{Q}$ if $\operatorname{Char} F = 0$. ☐

Definition 1.3. The intersection of all subfields of a field F is the *prime subfield* of F.

Date: September 2, 2005.

2. Extensions

Definition 2.1. Let F and K be fields with $F \subseteq K$. Then F is a *subfield* of K, and K is an *extension* of F. Observe that K is a vector space over F. If K is a finite dimensional vector space over F of dimension d then d is the *degree* of the extension, and is denoted $[K : F]$. We write $[K : F] < \infty$ to indicate that K is a finite extension of F.

Proposition 2.2. *Let F, K and L be fields with $F \subseteq K \subseteq L$. If $[L : F] < \infty$ then $[K : F] < \infty$, $[L : K] < \infty$, and $[L : F] = [K : F][L : K]$.*

Proof. Let $\mathcal{L} = (l_1, \dots, l_m)$ be an ordered basis of L as a vector space over F. Since $\mathcal{L}$ is a spanning set of L as a vector space over F, it is also a spanning set for L as a vector space over K. Thus $[L : K] \leq [L : F]$, and in particular L is a finite extension of K. Since K, viewed as a vector space over F, is a subspace of the finite dimensional vector space L, it follows that K is a finite extension of F. Choose an ordered basis $\mathcal{K} = (k_1, \dots, k_n)$ of K over F.

We will show that $(k_i l_j)$ is a basis of L over F, where i runs from 1 to n and j runs from 1 to m. To show that it is a spanning set, choose an arbitrary element l of L. Write $l = a_1 l_1 + \cdots + a_m l_m$, where $a_1, \dots, a_m \in K$. For each $i = 1, \dots, m$, write $a_i = b_{i1} k_1 + \cdots + b_{in} k_n$. Then we have

$$l = \sum_{i=1}^{m} (\sum_{j=1}^{n} b_{ij} k_i) l_j = \sum_{i=1}^{m} \sum_{j=1}^{n} b_{ij} k_i l_j.$$

This shows that $\mathcal{L}$ is a spanning set. To show that $\mathcal{L}$ is independent, suppose that

$$0 = \sum_{i=1}^{m} \sum_{j=1}^{n} b_{ij} k_i l_j = \sum_{i=1}^{m} (\sum_{j=1}^{n} b_{ij} k_i) l_j.$$

Since L is independent over K, we have $b_{i1} k_1 + \cdots + b_{in} k_n = 0$ for $i = 1, \dots, m$. Since $\mathcal{K}$ is a basis for K over F, this implies that $b_{ij} = 0$ for $i = 1, \dots, m$ and $j = 1, \dots, n$.

Thus we have $[K : F] = m$, $[L : K] = n$ and $[L : F] = mn$. $\square$

Definition 2.3. Let F and K be fields with $F \subseteq K$ and let $\alpha_1, \dots, \alpha_k \in K$. The intersection of all subfields of K which contain F and $\{\alpha_1, \dots, \alpha_k\}$ is denoted $F(\alpha_1, \dots, \alpha_k)$ and, according to Exercise 1.4, is a subfield of K.

Exercise 2.1. Let F and K be fields with $F \subseteq K$ and let α and β be elements of K. Show that $F(\alpha)(\beta) = F(\beta)(\alpha) = F(\alpha, \beta)$.

3. Algebraic extensions

Definition 3.1. Let F and K be fields with $F \subseteq K$. Let $f(x) = a_0 + \cdots + a_n x^n \in F[x]$. If $\alpha \in K$ then we define

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

If $f(x) \neq 0$ and $f(\alpha) = 0$ then α is a *root* of f.

Exercise 3.1. Let F and K be fields with $F \subseteq K$. A polynomial of degree n in $F[x]$ has at most n roots in K.

Proposition 3.2. *Let F and K be fields with $F \subseteq K$ and let α be an element of K. If $[K : F] < \infty$ then there is a non-zero polynomial $f(x)$ with degree at most $[K : F]$ such that $f(\alpha) = 0$.*

Proof. Set $n = [K : F]$. The $n+1$ elements $1, \alpha, \ldots, \alpha^n$ of the K must be linearly dependent over F, since K has dimension n as a vector space over F. Thus there exist elements $a_0, \ldots, a_n$ of F, not all equal to 0, such that $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. If we set $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ then we have $f(\alpha) = 0$. $\square$

Definition 3.3. Suppose that F and K are fields with $F \subseteq K$ and that α is an element of K. If there exists $f(x) \in F[x]$ such that $f(\alpha) = 0$ then α is *algebraic* over F. We may sometimes omit reference to the field K when referring to algebraic elements over F.

3.4. The set

$$A = \{f(x) \in F[x] \mid f(\alpha) = 0\}$$

is an ideal in the polynomial ring $F[x]$. Since $F[x]$ is a PID, the ideal A is generated by a single polynomial $g(x)$, which is unique up to multiplication by units. Thus there is a unique monic polynomial $g(x)$ which generates A. (A polynomial is *monic* if the non-zero coefficient of highest degree is equal to 1.) The unique monic generator of A is called the *minimal polynomial* of α over F. It may also be described as the monic polynomial of least degree having α as a root.

Exercise 3.2. Let F be a field and suppose that α is algebraic over F. Prove that the minimal polynomial if α is irreducible.

Proposition 3.5. *Suppose that α is algebraic over the field F. The degree of the minimal polynomial of α over F is equal to $[F(\alpha) : F]$.*

Exercise 3.3. Prove Proposition 3.5

Exercise 3.4. Let F and K be fields with $F \subseteq K$ and let $f \in F[x]$. For each $\alpha \in K$ the function $\phi_\alpha : F[x] \to K$ defined by $\phi_\alpha(f) = f(\alpha)$ is a ring homomorphism.

3.6. If F is a field and $f(x) \in F[x]$ is an irreducible polynomial then the quotient $F[x]/(f)$ is a field, and we have maps

$$F \longrightarrow F[x] \longrightarrow F[x]/(f)$$

where the map on the left sends each element a in F to the degree 0 polynomial a, and the map on the right is the natural surjection. The composition of these two maps is an injection from F to the field $F[x]/(f)$. We will always identify F with its image under this injection, so that the field $F[x]/(f)$ can be regarded as an extension of F.

Definition 3.7. An *embedding* of a field F into a field K is a non-zero homomorphism from F to K. (Any non-zero field homomorphism is injective since a field has no proper ideals.) If K is an extension of a field F and $\eta : F \to L$ is an embedding, then an embedding $\hat{\eta} : K \to L$ is called an *extension* of η provided that $\hat{\eta}|_F = \eta$.

Exercise 3.5. Suppose that $\eta : F \to K$ is an embedding of fields. Let $\tilde{\eta} : F[x] \to K[x]$ be defined by

$$\tilde{\eta}(a_0 + \cdots + a_n x^n) = \eta(a_0) + \cdots + \eta(a_n)x^n.$$

Prove that $\tilde{\eta}$ is an injective ring homomorphism.

Exercise 3.6. Suppose that F is a field and $f(x) \in F[x]$ is irreducible, so that $F[x]/(f)$ is a field. Let $\bar{x}$ denote the coset of the polynomial x in the quotient $F[x]/(f)$. Prove that $\bar{x}$ is a root of f in the field $F[x]/(f)$.

Proposition 3.8. *Let F be a field. Let $f(x) \in F[x]$ be an irreducible polynomial and let $\bar{x}$ denote the coset of the polynomial x in the extension field $F[x]/(f)$ of F (see 3.6). Suppose that $\eta : F \to K$ is an embedding of F into a field K. Any extension of η to an embedding of $F[x]/(f)$ into L must send $\bar{x}$ to a root of $f(x)$. If α is any root of $f(x)$ in L then there exists an extension $\eta_\alpha : F[x]/(f) \to L$ such that $\eta_\alpha(\bar{x}) = \alpha$ and the image of η_α is $\eta(F)(\alpha)$.*

Proof. We use the notation of Exercise 3.5.

Suppose that $\hat{\eta}$ is an extension of η to an embedding of $F[x]/(f)$ into K. If $f(x) = a_0 + \cdots a_n x^n$ then, since $\bar{x}$ is a root of $f(x)$ in $F[x]/(f)$,

$$0 = \hat{\eta}(a_0 + \cdots a_n \bar{x}^n) = \hat{\eta}(a_0) + \cdots + \hat{\eta}(a_n)\hat{\eta}(\bar{x}) = \eta(a_0) + \cdots + \eta(a_n)\eta(\bar{x}).$$

Thus any extension of η must send $\bar{x}$ to some root of $\tilde{\eta}(f)$.

For any $\alpha \in K$ we can consider the homomorphism $\tilde{\eta} \circ \phi_\alpha : F[x] \to K$. That is, $\tilde{\eta} \circ \phi_\alpha(f)$ is the element of K obtained by evaluating the polynomial $\tilde{\eta}(f)$ at α. Observe that $\tilde{\eta} \circ \phi_\alpha(\bar{x}) = \alpha$. If we assume, in addition, that the element $\alpha \in K$ is a root of $\tilde{\eta}(f)$ then the kernel of $\tilde{\eta} \circ \phi_\alpha$ is the ideal (f). Thus, by the first isomorphism theorem, we obtain an embedding η_α of the field $F[x]/(f)$ into K such that $\eta_\alpha(\bar{x}) = \alpha$ and $\eta_\alpha|_F = \eta$, where we are regarding F as a subfield of $F[x]/(f)$ as in 3.6. Since the image of η_α contains α, and is clearly contained in the field generated by $\eta(F)$ and α, we see that the image of η_α is $\eta(F)(\alpha)$. □

Corollary 3.9. *Let F be a field and K an extension of F. Suppose that $\alpha \in K$ is algebraic over the field F. Let $f(x)$ be the minimal polynomial of α over F. Then the field $F(\alpha) \subseteq K$ is isomorphic to $F[x]/(f(x))$ by an isomorphism that restricts to the identity on F.*

Definition 3.10. Suppose the field K is an extension of the field F. Then K is an *algebraic extension* of F if every element of K is algebraic over F.

Exercise 3.7. Show that any finite extension is algebraic.

Proposition 3.11. *Suppose that F, K and L are fields, with $F \subseteq K \subseteq L$. If K is an algebraic extension of F and L is an algebraic extension of K, then L is an algebraic extension of F.*

Proof. Let α be an element of the field L. Since α is algebraic over K, there is a polynomial $f(x) \in K[x]$ such that $f(\alpha) = 0$. Suppose that $f(x) = a_0 + \cdots + a_n x^n$, where $a_0, \ldots, a_n \in K$. Consider the field $H = F(a_0, \ldots, a_n)$. Clearly α is algebraic over H, and H is a finite extension of F since each of $a_0, \ldots, a_n$ is algebraic over F. Thus $H(\alpha)$ is a finite extension of F. Since any element of a finite extension is algebraic, we have shown that α is algebraic over F. Since α was arbitrary, L is an algebraic extension of F. □

Proposition 3.12. *Suppose that F and K are fields with $F \subseteq K$. The set of elements of K which are algebraic over F forms a subfield of K.*

Proof. We need only show that the set of algebraic elements is closed under the operations. If α is algebraic over F then $F(\alpha)$ is a finite extension of F, and hence any element of $F(\alpha)$ is algebraic over F. In particular, if $\alpha \neq 0$ then α^{-1} is algebraic. Similarly, if α and β are algebraic over F then $\alpha + \beta$ and $\alpha\beta$ are elements of the finite extension $F(\alpha, \beta)$ of F, and consequently are algebraic. □

4. Splitting fields

Definition 4.1. Let F be a field and let $f(x)$ be a non-constant polynomial in $F[x]$. The polynomial f *splits over* K if f factors as a product of linear polynomials in $K[x]$.

Theorem 4.2. *Given any field F and any non-constant polynomial $f(x) \in F[x]$, there exists a finite extension K of F such that f splits over K.*

Proof. Let $n \geq 1$ be the degree of f. Let K be chosen among all finite extensions F so that the number k of irreducible factors of $f(x)$ in $K[x]$ is as large as possible. If $k = n$ then each factor must be linear, so f splits over K. If $k < n$ then there is an irreducible factor $g(x) \in K[x]$ of $f(x)$ such that the degree of g is at least 2. The field $L = K[x]/(g)$ is a finite extension of K in which g has a root, and hence in which g factors. But then f has more irreducible factors in $L[x]$ than it has in $F[x]$, contradicting the choice of K. $\square$

Definition 4.3. An extension K of F is a *splitting field* for f provided that f splits over K and f does not split over any proper subfield of K.

4.4. Every non-constant polynomial in $F[x]$ has a splitting field K. Specifically, if L is a finite extension of K such that $f(x)$ splits over L, then we may take K to be the intersection of all subfields of L over which f splits.

Proposition 4.5. *Let F be a field and let $f(x)$ be a non-constant polynomial in $F[x]$. Suppose that L is an extension of F such that f splits over L. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in L. Then $F(\alpha_1, \ldots, \alpha_n)$ is a splitting field for f, and any splitting field for f is isomorphic to $F(\alpha_1, \ldots, \alpha_n)$.*

Proof. Clearly f splits over $F(\alpha_1, \ldots, \alpha_n)$. On the other hand, if H is any proper subfield of L containing F, then there exists some index i such that α_i is not contained in H. The minimal polynomial of α_i over H is an irreducible factor of f in $H[x]$ and also has degree greater than 1. Therefore f does not split over H. This shows that $F(\alpha_1, \ldots, \alpha_n)$ is a splitting field for f.

Now let K be a splitting field for f. Let C be an algebraic closure of L. We know from Proposition 6.8 that there exists an embedding σ of K/F into C. We need only show that $\sigma(K) = F(\alpha_1, \ldots, \alpha_k) \subseteq L$.

Any root of f in K must map to a root of f in C. Thus $F(\alpha_1, \ldots, \alpha_k) \subseteq \sigma(K)$. Since σ is an isomorphism from K to $\sigma(K)$, we know that f cannot split over any proper subfield H of $\sigma(K)$. On the other hand, f does split over $F(\alpha_1, \ldots, \alpha_k)$. It follows that $\sigma(K) = F(\alpha_1, \ldots, \alpha_k)$. $\square$

Corollary 4.6. *Let F be a field and let $f(x)$ be a non-constant polynomial in $F[x]$. Any two splitting fields for f are isomorphic.*

Corollary 4.7. *If F and F' are finite fields of the same order then F is isomorphic to F'*

Proof. Let F be a finite field. The order of F is p^k for some prime p and some positive integer k. Since the multiplicative group of non-zero elements of F has order $p^k - 1$, every element of F is a root of the polynomial $f(x) = x^{p^k} - x$. On the other hand, since

f has degree p^k, it has at most p^k roots. This shows that F is a splitting field for f. So is F'. Therefore $F \cong F'$. □

Exercise 4.1. Let G be a finite abelian group. Use the structure theorem for finite abelian groups to show that if there are at most n elements of order n in G, for all positive integers n, then G is cyclic.

Exercise 4.2. Let F be a field and let G be a finite subgroup of $F^\times$, the multiplicative group of non-zero elements of F. Show that G is cyclic. In particular, if F is a finite field then $F^\times$ is a cyclic group.

5. Algebraic closures

We will first prove the Fundamental Theorem of Algebra, assuming that the field of real numbers has been constructed, and is known to be a connected topological space. Specifically, we assume the result from calculus, based on the Intermediate Value Theorem, which says that every odd degree polynomial in $\mathbb{R}[x]$ has a real root. We define the complex numbers $\mathbb{C}$ to be $\mathbb{R}(i)$ where i is a root of x^2+1; no topological properties of $\mathbb{C}$ will be needed for this proof.

Lemma 5.1. *Suppose that F and K are fields with $F \subseteq K$. Let α and β be elements of an extension L of K. If there exist two distinct elements $s, t \in F$ such that $\alpha + s\beta \in K$ and $\alpha + t\beta \in K$ then $F(\alpha, \beta) \subseteq K$.*

Proof. Subtracting, we have $(s-t)\beta \in K$. Since $s \neq t$, this implies that $\beta \in K$. But then $s\beta \in K$, so $\alpha = (\alpha + s\beta) - s\beta \in K$. □

Theorem 5.2 (The Fundamental Theorem of Algebra)**.** *Every non-constant polynomial in $\mathbb{C}[x]$ splits over $\mathbb{C}$.*

Proof. It suffices to show that every polynomial of positive degree in $\mathbb{C}[x]$ has a root in $\mathbb{C}$. For this, it suffices to show that every polynomial in $\mathbb{R}[x]$ has a root in $\mathbb{C}$, since if $f(x) \in \mathbb{C}[x]$ had no roots in $\mathbb{C}$, then $\overline{f}(x)$ would also have no roots in $\mathbb{C}$, and hence $f(x)\overline{f}(x)$, being equal to its own conjugate, would be a polynomial in $\mathbb{R}[x]$ with no roots in $\mathbb{C}$.

We show by induction on n that any real polynomial of degree $2^n m$, m odd, has a root in $\mathbb{C}$. The case $n=0$ follows from the calculus theorem mentioned above. For the induction step, suppose that $f(x) \in \mathbb{R}[x]$ has degree $2^n m$, m odd. Let K be a splitting field for f over $\mathbb{C}$. Let $\alpha_1, \dots, \alpha_k$ be the roots of f in K. For any real number t, let

$$g_t(x) = \prod_{0<i<j\leq k} (x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j)).$$

Notice that the degree of g_t is $2^n m(2^n m - 1)/2 = 2^{n-1}(2^n m - 1)$, and $2^n m - 1$ is odd. Therefore, by induction, each g_t has a root in $\mathbb{C}$. So for any real number t there exist integers $0 < i < j \le k$ such that $\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbb{C}$. Since there are infinitely many real numbers and only finitely many pairs i, j, there must exist real numbers s and t, with $s \neq t$, and a pair i, j so that both of the elements $\alpha_i + \alpha_j + s\alpha_i\alpha_j$ and $\alpha_i + \alpha_j + t\alpha_i\alpha_j$ of K are contained in $\mathbb{C}$. By Lemma 5.1, this implies that $\alpha_1 + \alpha_2 \in \mathbb{C}$ and $\alpha_1\alpha_2 \in \mathbb{C}$. In particular the coefficients of the polynomial $(x - \alpha_1)(x - \alpha_2)$ are contained in $\mathbb{C}$. But the quadratic formula shows that any quadratic polynomial in $\mathbb{C}[x]$ has roots in $\mathbb{C}$. That is, α_1 and α_2 are in $\mathbb{C}$. This completes the induction step. □

Theorem 5.3 (Artin's construction)**.** *Let F be a field. There exists an extension F_1 of F such that every polynomial in $F[x]$ has a root in F_1.*

Proof. It suffices to construct an extension F_1 such that every monic irreducible polynomial has a root in F_1.

Let P be the set of monic irreducible polynomials in $F[x]$. For each $f(x) \in P$, let x_f be an indeterminate, and set $\mathcal{X} = \{x_f \mid f(x) \in P\}$. Let $F[\mathcal{X}]$ denote the ring of polynomials in the indeterminates $\mathcal{X}$. For each $f(x) \in P$, let $\hat{f}$ be the polynomial in $F[\mathcal{X}]$ obtained by substituting x_f for x. Let A be the ideal generated by $\{\hat{f} \mid f(x) \in P\}$. We claim that A is a proper ideal. Otherwise, we could write $1 = g_1\hat{f}_1 + \cdots g_k\hat{f}_k$ where $f_1(x), \ldots, f_k(x) \in P$ and $g_1, \ldots, g_k \in R[\mathcal{X}]$. Let K be a finite extension of F which contains a root α_i of $f_i(x)$ for $1, \ldots, k$. Then $F[\mathcal{X}]$ is a subring of $K[\mathcal{X}]$. Since the equation $1 = g_1\hat{f}_1 + \cdots g_k\hat{f}_k$ holds in $K[\mathcal{X}]$, if we substitute elements of K for indeterminates we will obtain a valid equation in K. But if we substitute α_i for x_{f_i} and 0 for each of the other indeterminates in $\mathcal{X}$ then we obtain the absurd equation $1 = 0$ in K. This contradiction shows that A is a proper ideal and therefore, by Zorn's Lemma, is contained in a maximal ideal M. Consider the field $F_1 = F[\mathcal{X}]/M$. For each polynomial $f(x) \in P$ the element x_f is sent under the natural map to a root of f in F_1. We may embed F into F_1 as the image of the degree 0 polynomials under the natural map. Thus F_1 is an extension of F which contains a root of every polynomial in $F[x]$. □

Definition 5.4. A field K is *algebraically closed* if every polynomial in $K[x]$ has a root in K.

In particular, $\mathbb{C}$ is algebraically closed.

Exercise 5.1. Show that if K is algebraically closed, then every polynomial in $K[x]$ factors as a product of linear polynomials.

Proposition 5.5. *Let F be a field. Then F has an algebraically closed extension.*

Proof. Let F_1 be the extension given by Artin's construction. Thus every polynomial in $F[x]$ has a root in F_1. It is not necessarily the case that every polynomial in $F_1[x]$ has a root in F_1. So we may apply Artin's construction to F_1 to obtain an extension F_2 of F_1 such that every polynomial in $F_1[x]$ has a root in F_2. Repeating, we obtain an infinite sequence of fields $F = F_0 \subseteq F_1 \subseteq \cdots$ such that every polynomial in $F_i[x]$ has a root in F_{i+1}. Let $\mathcal{F}$ be the union of the F_i. If x and y are elements of $\mathcal{F}$ then there exists an integer i such that x and y are both contained in F_i; the sum and product of x and y are defined to be their sum and product as elements of F_i. It is not hard to see that this makes $\mathcal{F}$ into an extension field of F.

If $f(x)$ is any polynomial in $\mathcal{F}[x]$ then there exists an integer i such that all of the coefficients of $f(x)$ are contained in F_i. Thus $f(x)$ has a root in $F_{i+1} \subseteq \mathcal{F}$. This shows that $\mathcal{F}$ is algebraically closed. □

Definition 5.6. An extension K of a field F is an *algebraic closure* of F if K is an algebraic extension of F and K is algebraically closed.

5.7. Observe that if C is an algebraic closure of F then no proper subfield of C can be an algebraic closure of F. If K is a proper subfield of C and $\alpha \in C - K$ then K clearly does not contain all of the roots of the minimal polynomial of α, so it is not algebraically closed.

On the other hand, if C is an algebraic closure of F and K is a subfield of C with $F \subseteq K \subseteq C$ then C is an algebraic closure of K.

The field $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$, since any algebraically closed extension of $\mathbb{R}$ must contain a root of $x^2 + 1$.

Theorem 5.8. *Any field has an algebraic closure.*

Proof. Let $\mathcal{F}$ be an algebraically closed extension of F. Let $K \subseteq \mathcal{F}$ denote the set of elements of $\mathcal{F}$ which are algebraic over F. This is a subfield of $\mathcal{F}$ by Proposition 3.12, and is clearly an algebraic extension of F. To show that K is algebraically closed, consider a polynomial $f(x) = a_0 + \cdots + a_n x^n$ in $K[x]$. Let $\alpha \in \mathcal{F}$ be a root of f. Since $K(\alpha)$ is an algebraic extension of K and K is an algebraic extension of F, Proposition 3.11 shows that $K(\alpha)$ is algebraic over F. In particular, α is algebraic over F and hence is contained in K. This shows that K is algebraically closed. □

Proposition 5.9. *Let F be field. Suppose that K and K' are extensions of F and that $\phi : K \to K'$ is an isomorphism which restricts to the identity on F. Let $f(x) \in K[x]$ be an irreducible polynomial and define $\tilde{\phi}(f) \in K'[x]$ as in Exercise 3.5. Suppose that L and L' are extensions of K and K' respectively, such that L contains a root α of f and*

L' contains a root α' of $\tilde{\phi}(f)$. Then there is an isomorphism $\hat{\phi} : K(\alpha) \to K'(\alpha')$ which restricts to ϕ on K.

Exercise 5.2. Use Proposition 3.8 to Prove Proposition 5.9.

Theorem 5.10. *If C and C' are two algebraic closures of a field F then there is an isomorphism from C to C' which fixes F.*

Proof. The proof is based on Zorn's Lemma. Let X be the set of all injective homomorphisms $\phi : K \to C'$ where $K \subseteq C$ is an extension of F and where ϕ restricts to the identity on F. If $\phi : H \to C'$ and $\psi : K \to C'$ are elements of X, define $\phi \leq \psi$ if $H \subseteq K$ and $\psi|_H = \phi$. This is easily seen to be a partial ordering on X.

We claim that any chain in X has an upper bound. If $Y \subseteq X$ is a chain, then the family $\{\operatorname{dom}\phi \,|\, \phi \in Y\}$ is a nested family of subfields of C. Let H denote the union of all of these subfields, which is a subfield of C. Define $\Phi : H \to C'$ as follows. If $\alpha \in H$ then there is an element $\phi : K \to C'$ in Y such that $\alpha \in K$. Set $\Phi(\alpha) = \phi(\alpha)$. Since any two homomorphisms in Y agree on the intersection of their domains, the homomorphism Φ is well defined, and is clearly an upper bound for Y.

Thus by Zorn's lemma there exists a maximal element $\phi : K \to C'$ in Y. We will show that $K = C$. If not, choose $\alpha \in C - K$. Since C is an algebraic extension of F, it is also an algebraic extension of K; set $K' = \phi(K) \subseteq C'$. Let $f(x) \in K[x]$ be the minimal polynomial of α and define $\tilde{\phi}(f) \in K'[x]$ as in Exercise 3.5. Let $\alpha' \in C'$ be a root of $\tilde{\phi}(f)$. By Proposition 5.9 there is an isomorphism $\hat{\phi}$ from $K(\alpha)$ to $K'(\alpha')$ which restricts to ϕ on K. But then $\phi : K \to C'$ is less than $\hat{\phi} : K(\alpha) \to C'$ in the ordering of Y, which contradicts the maximality of ϕ. Thus we have $K = C$. Since $\phi(K)$ is isomorphic to K it is also algebraically closed, so we must have $\phi(K) = C'$. □

6. Embeddings

Definition 6.1. If the field L is an extension of F, then an *embedding of K/F into L* is an embedding of K in L which restricts to the identity on F. The set of all embeddings of K/F into L will be denoted $\operatorname{Emb}(K/F, L)$.

The goal of this section is to count the number of embeddings of K/F into C in the case where K is a finite extension of F and C is an algebraically closed extension of F.

Theorem 6.2. *Let F be a field and let C be an algebraically closed extension of F. Suppose that K and L are finite extensions of F with $F \subseteq K \subseteq L$ Then every embedding of K/F into C extends to an embedding of L/F into C.*

Proof. The proof is by strong induction on $[L : K]$. The case $[L : K] = 1$ is obvious since $K = L$ in that case. Suppose that σ is an embedding of K/F in C. Choose an element $\alpha \in L - K$. Proposition 5.9 implies that σ extends to an embedding σ' of $K(\alpha)/F$ into C. Since $[L : K(\alpha)] < [L : K]$, the induction hypothesis implies that σ' extends to an embedding of L/F into C. This is also an extension of σ, since σ' is an extension of σ. ☐

6.3. Suppose that F is a field and K is any finite extension of F. We can construct K from F by forming a finite sequence of simple algebraic extensions. Choose $\alpha_1 \in K - F$. Since $\alpha_1 \notin K$, we have $[F(\alpha_1) : F] > 1$. (The minimal polynomial of α_1 has degree 1 only if $\alpha_1 \in F$.) Thus $[K : F(\alpha_1)] = [K : F]/[F(\alpha_1)] < [K : F]$. Next choose $\alpha_2 \in K - F(\alpha_1)$. Continuing this process we obtain fields

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq \cdots .$$

Since $[K : F(\alpha_1, \ldots, \alpha_i)] < [K : F(\alpha_1, \ldots, \alpha_{i-1})]$, we must have $F(\alpha_1, \ldots, \alpha_k) = K$ for some $k \leq [K : F]$. (In fact, since each of these degrees divides $[K : F]$, we have $k < [K : F]$.)

Lemma 6.4. *Let F be a field and let $f(x)$ be an irreducible polynomial in $F[x]$. Suppose that $\eta : F \to K$ is an embedding of F into K. The number of distinct extensions of η to embeddings of $F[x]/(f)$ into K is equal to the number of distinct roots of $f(x)$ in K.*

Proof. This follows immediately from Proposition 3.8. ☐

Proposition 6.5. *Suppose that K is a finite extension of a field F. Let C be an algebraically closed extension of F. Suppose that $K = F(\alpha_1, \ldots, \alpha_k)$. For each $i = 1, \ldots, k$ let $f_i(x) \in F(\alpha_1, \ldots, \alpha_{i-1})[x]$ be the minimal polynomial of α_i. Suppose that f_i has n_i roots in C. Then $|\operatorname{Emb}(K/F, C)| = n_1 \cdots n_k \leq [K : F]$.*

Proof. The proof is by induction on k. For the case $k = 1$ observe that Proposition 3.8 shows that the number of embeddings of $F[x]/(f_1)$ into K which restrict to the identity on F is equal to the number of distinct roots of $f_1(x)$ in K. Fix an isomorphism from $\phi : F(\alpha_1) \to F[x]/(f_1)$. A homomorphism $\eta : F[x]/(f_1) \to K$ is an embedding of $F[x]/(f_1)$ into K which restricts to the identity on F if and only if $\eta \circ \phi$ is an embedding of $F(\alpha_1)/F$ into K. Thus there are n_1 of these.

By Theorem 6.2, each of the n_1 embeddings of $F(\alpha_1)/F$ into C extends to an embedding of K/F into C. Suppose that η is an embedding of $F(\alpha_1)/F$ into C and that $\hat{\eta}$ is an extension of η to an embedding of K/F into C. If we set $\alpha'_i = \hat{\eta}(\alpha_i)$ then, since $\hat{\eta}$ is an isomorphism, the minimal polynomial of α'_i over the field $F(\alpha'_1, \ldots, \alpha'_{i-1})$ has the same number of roots in $\hat{\eta}(K)$ as f_i has in K. Thus, by induction, there are $n_2 \cdots n_k$ embeddings of $\hat{\eta}(K)/\eta(F(\alpha_1))$ into C. But a homomorphism τ is an embedding of $\hat{\eta}(K)/\eta(F(\alpha_1))$

into C if and only if $\tau \circ \eta$ is an embedding of K/F into C which restricts to eta on $F(\alpha_1)$. Thus there are $n_2 \cdots n_k$ extensions of η to embeddings of K/F into C. Since there are n_1 choices for η, It follows that there are a total of $n_1 \cdots n_k$ embeddings of K/F in C. $\square$

Definition 6.6. Let F be a field. A polynomial $f(x)$ of degree n in $F[x]$ is *separable* if it has n distinct roots in some extension of F. An algebraic extension K of F is *separable* if every element of K has a separable minimal polynomial over F.

Exercise 6.1. Show that a polynomial $f(x) \in F[x]$ of degree n is separable if and only if f has n distinct roots in any algebraic closure of F.

With the notion of a separable polynomial in hand we can state the following corollary of Proposition 6.5.

Corollary 6.7. *Let F be a field and suppose that $f(x) \in F[x]$ is a separable polynomial of degree n. Let $\alpha_1, \ldots, \alpha_n$ be the distinct roots of f in some extension C of F, and set $K = F(\alpha_1, \ldots, \alpha_n)$. Then $|\operatorname{Emb}(K/F, C)| = [K : F]$.*

Proof. Since the degree $[K : F]$ is equal to the product of the degrees of the polynomials f_i in the Proposition, it suffices to show that each f_i is separable, since we will then know that its degree is equal to the number n_i of its roots. Each polynomial f_i is contained in $H[x]$ for some field H with $F \subseteq H \subseteq K$, and f_i divides f in $H[x]$. Thus f_i divides f in $K[x]$. But the prime power factors of f in $K[x]$ are the distinct linear polynomials $x - \alpha_i$, for $i = 1, \ldots, n$, each appearing with exponent 1 in the factorization of f. Since the monic polynoial f_i divides f, it cannot have repeated roots. $\square$

Exercise 6.2. Let F, K and L be fields, with $F \subseteq K \subseteq L$. Show that if L is a separable extension of F then L is a separable extension of K.

Theorem 6.8. *If K is a finite separable extension of F and C is an algebraically closed extension of F then $|\operatorname{Emb}(K/F, C)| = [K : F]$.*

Proof. Write $K = F(\alpha_1, \ldots, \alpha_k)$. Let $f_i(x)$ be the minimal polynomial of α_i over $F(\alpha_1, \ldots, \alpha_{i-1})$. By Exercise 6.2 each f_i is separable. Let n_i be the degree of f_i, which is equal to the number of roots of f_i in C. Now we have

$$[K : F] = [F(\alpha_1) : F] \cdots [F(\alpha_1, \ldots, \alpha_k) : F(\alpha_1, \ldots, \alpha_{k-1})] = n_1 \cdots n_k = |\operatorname{Emb}(K/F, C)|,$$

where the last equality follows from Proposition 6.5. $\square$

7. Separability

Definition 7.1. A field F is *perfect* if every algebraic extension of F is separable.

The key to understanding how an algebraic extension can fail to be separable is the algebraic notion of the derivative of a polynomial.

Definition 7.2. Let F be a field and let $f(x) = a_0 + a_1 x + \cdots a_n x^n$ be a polynomial in $F[x]$. The *derivative* of f is the polynomial $f'(x) = a_1 + \cdots n a_n x^{n-1}$.

Exercise 7.1. Let F be a commutative ring. Show that if $f(x)$ and $g(x)$ are two polynomials in $F[x]$ then $(f+g)' = f' + g'$ and $(fg)' = f'g + fg'$.

7.3. Observe that if F is field with non-zero characteristic then it is possible for a non-constant polynomial in $F[x]$ to have derivative 0. For example, consider $f(x) = x^2 + 1 \in \mathbb{F}_2[x]$. We have $f'(x) = 2x = 0$. On the other hand, if $\operatorname{Char} f = 0$ then a polynomial of degree at least 1 cannot have derivative 0.

Proposition 7.4. *Let F be field and let $f(x) \in F[x]$ be an irreducible polynomial. If $f(x)$ is not separable then $f'(x) = 0$.*

Proof. Suppose that $f(x)$ is not separable and that $f'(x) \neq 0$. Since $f(x)$ is irreducible, and $f'(x)$ has lower degree than $f(x)$, the greatest common divisor of f and f' is 1. Let $a(x)$ and $b(x)$ be polynomials in $F[x]$ such that $a(x)f(x) + b(x)f'(x) = 1$.

Since f is not separable, there is an extension K of F such that f has a repeated root $\alpha \in K$. Thus in $K[x]$ we have $f(x) = (x-\alpha)^2 h(x)$. By the product rule, $f'(x) = 2(x-\alpha)h(x) + (x-\alpha)^2 h'(x)$. Thus $f(\alpha) = f'(\alpha) = 0$.

Since the equation $a(x)f(x) + b(x)f'(x) = 1$ holds in $F[x]$, it also holds in $K[x]$ when we regard a, b, f and f' as polynomials in $K[x]$. But this is absurd since $a(\alpha)f(\alpha) + b(\alpha)f'(\alpha) = 0$ in $K[x]$. This contradiction shows that $f'(x) = 0$. □

Proposition 7.5. *Let F be field and let $f(x) \in F[x]$ be a polynomial of positive degree. If $f'(x) = 0$ then $\operatorname{Char} F = p$ for some prime p and $f(x) = g(x^{np})$ for some $n > 0$ and some polynomial $g(x)$ with $g'(x) \neq 0$. In particular, if f is monic and irreducible, but not separable, then $f(x) = g(x^{np})$ where $n > 0$ and g is monic, irreducible and separable.*

Proof. Suppose that $f'(x) = 0$. Write $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Consider a monomial $a_k x^k$ where $a_k \neq 0$. Since $f'(x) = 0$ we have $k a_k x^k = 0$, so F must have non-zero characteristic p and k must be divisible by p. Thus the non-zero monomials in f all have degree divisible by p. Let np be the greatest common divisor of the degrees of the non-zero monomials that occur in f. We have $f(x) = g(x^{np})$, where the coefficients of g are the same as those of f, but of different degree. There is at least one non-zero monomial in g with degree not divisible by p. Thus $g'(x) \neq 0$. Any factorization of g yields a factorization of f by substituting x^{np} for x. Thus g is irreducible whenever f is irreducible. □

Corollary 7.6. *A field of characteristic 0 is perfect.*

Proposition 7.7. *Let F be a field of characteristic $p \neq 0$. Suppose that a and b are elements of F. Then $(a+b)^p = a^p + b^p$. In particular, the function $\Phi_F : F \to F$ defined by $\Phi_F(x) = x^p$ is a homomorphism.*

Proof. Expand $(a+b)^p$ using the binomial theorem. All of the binomial coefficients are divisible by p, except for the first and last ones. □

Definition 7.8. If R is a ring of characteristic p, the homomorphism $\Phi_F : F \to F$ given by $\Phi_F(x) = x^p$ is called the *Frobenius endomorphism* of F.

Lemma 7.9. *Let F be a field of characteristic $p \neq 0$. If the Frobenius endomorphism Φ_F is surjective, then $g(x^p)$ is in the image of the Frobenius endomorphism $\Phi_{F[x]}$ for any polynomial $g(x) \in F[x]$.*

Proof. Write $g(x) = a_0 + \cdots + a_n x^n$. For each $i = 0, \ldots, n$ choose $b_i \in F$ such that $b_i^p = a_i$. Set $h(x) = b_0 + \cdots + b_n x^n$. We have

$$\begin{aligned} h(x)^p &= (b_0 + b_1 x + \cdots + b_n x^n)^p \\ &= b_0^p + b_1^p x^p + \cdots + b_n^p x^{np} \\ &= a_0 + a_1 x^p + \cdots + a_n x^{np} = g(x^p). \end{aligned}$$

Thus $g(x^p)$ is the image of $h(x)$ under the Frobenius endoomorphism of $F[x]$. □

Proposition 7.10. *If F is a field of characteristic $p \neq 0$ and if the Frobenius endomorphism $\Phi_F : F \to F$ is surjective, then F is perfect.*

Proof. Let F be a perfect field and consider a monic irreducible polynomial $f(x) \in F[x]$ of degree m. Suppose that $f(x)$ is not separable. Then, according to Propositions 7.4 and 7.5 we must have $\operatorname{Char} F = p \neq 0$ and we can write $f(x) = g(x^{np})$ for some separable polynomial g. A polynomial in x^{np} can also be regarded as a polynomial in x^p, so Lemma 7.9 implies that $f(x) = h(x)^p$ for some polynomial $h(x) \in F[x]$. This contradicts the irreducibility of f. □

Corollary 7.11. *Any finite field is perfect.*

Proof. An endomorphism of a field is always injective. An injective map from a finite set to itself is surjective. Thus the Frobenius homomorphism of a finite field is surjective. □

Example 7.12. The field $\mathbb{F}_2(t)$ of rational functions with coefficients in $\mathbb{F}_2$ is not perfect.

To prove that $\mathbb{F}_2(t)$ is not perfect it suffices to show that the polynomial $f(x) = x^2 - t$ has no root in $\mathbb{F}_2(t)$. That is, there is no square root of t in $\mathbb{F}_2(t)$. This implies that f is irreducible. But there is an algebraic extension K of $\mathbb{F}_2(t)$ which contains a square root of t. If we denote this element of K by $\sqrt{t}$ then in $K[x]$ we have $f(x) = x^2 - t = x^2 + t = (x + \sqrt{t})^2$, so f is an irreducible polynomial of degree 2 in $\mathbb{F}_2(t)[x]$ which has only one root in the algebraic extension K of $\mathbb{F}_2(t)$.

A proof that there is no square root of t in $\mathbb{F}_2(t)$ is similar to Euclid's proof that the square root of 2 is irrational. Suppose there is a rational function $p(t)/q(t)$ whose square is t. We may assume that $p(t)$ and $q(t)$ are relatively prime. We have $p(t)^2 = tq(t)^2$. Since t is an irreducible polynomial, and hence is prime, t must divide p. If we set $p(t) = tr(t)$ then we have $t^2r(t)^2 = tq(t)$, so $tr(t) = q(t)$. Thus t divides q as well, contradicting the assumption that p and q are relatively prime.

8. Normal Extensions

Definition 8.1. Let F be a field and K an extension of F. The group of automorphisms of K which restrict to the identity on F is denoted $\mathrm{Aut}(K/F)$. If G is any subgroup of $\mathrm{Aut}(K/F)$ then $\mathrm{Fix}(G) = \{k \in K \mid \sigma(k) = k \text{ for all } \sigma \in G\}$. It is easy to see that $\mathrm{Fix}(G)$ is a subfield of K containing F.

Theorem 8.2. *Let F be a field and K an extension of F. Suppose that G is a finite subgroup of* $\mathrm{Aut}(K/F)$. *Then* $[K : \mathrm{Fix}(G)] = |G|$.

Proof. Set $n = |G|$ and $m = [K : F]$.

We may assume that K is embedded in an algebraically closed field C. Each element of $\mathrm{Aut}(K/F)$ is an embedding of K/F into C. Thus

$$n = |G| \leq |\,\mathrm{Aut}(K/F, C)| \leq |\,\mathrm{Emb}(K/F, C)| \leq [K : F] = m.$$

Now write $G = \{\sigma_1, \ldots, \sigma_n\}$ and let $(\alpha_1, \ldots, \alpha_m)$ be a basis for K as a vector space over F. Consider the $n \times m$ matrix $A = [\sigma_i(\alpha_j)]$.

Since G is a group, it follows that for any $\sigma \in G$ we have $G = \{\sigma\sigma_1, \ldots, \sigma\sigma_n\}$. This means that the effect of applying σ to each entry of A is simply to permute the rows of A. Permuting the rows of a matrix does not change its null space, so if v is a column vector in K^n then $Av = 0$ if and only if $\sigma(A)v = 0$. On the other hand, since σ is a field automorphism we have that $Av = 0$ if and only if $\sigma(A)\sigma(v) = 0$. Combining these two statements we see that the null space of A is invariant under σ for any $\sigma \in G$.

Suppose that $n < m$. Then there is a non-zero column vector $v \in K^n$ such that $Av = 0$. We may assume that v has been chosen among all such vectors so that it has the minimal number of non-zero entries. After multiplying by the inverse of a non-zero entry we may also assume that v has one entry equal to 1.

Note that the row of A corresponding to the identity element of G contains the basis elements $\alpha_1, \dots, \alpha_m$. Since these are independent over $\mathrm{Fix}(G)$, a non-zero vector v with $Av = 0$ cannot have all of its entries contained in $\mathrm{Fix}(G)$. Thus v has an entry, say β, which is not contained in $\mathrm{Fix}(G)$.

Since β is not contained in $\mathrm{Fix}(G)$, there exists $\sigma \in G$ such that $\sigma(\beta) \neq \beta$. Now consider the vector $w = v - \sigma(v)$. Since the null space of A is invariant under G, the vector w also satisfies $Aw = 0$. Since $\sigma(\beta) \neq \beta$, there is at least one non-zero entry of w. But of course $\sigma(1) - \sigma(1) = 0$ and $\sigma(0) - \sigma(0) = 0$. Thus w has a zero entry in every position where v has either 0 or 1. This implies that w has fewer non-zero entries than v. This is a contradiction, so we must have $m = n$. □

Theorem 8.3. *Let F be a field and let K be a finite extension of F. The following are equivalent:*

(1) K is a splitting field of a separable polynomial in $F[x]$;

(2) $|\mathrm{Aut}(K/F)| = [K : F]$;

(3) $\mathrm{Fix}(\mathrm{Aut}(K/F)) = F$;

(4) if an irreducible polynomial $f(x) \in F[x]$ has a root in K then f is separable and splits over K;

(5) K is a separable extension of F and every embedding η of K/F into an algebraically closed extension of K satisfies $\eta(K) = K$.

Proof. ($1 \Rightarrow 2$) Let C be an algebraic closure of F. By Proposition 4.5 every embedding of K/F into C has the same image, namely $F(\alpha_1, \dots, \alpha_n)$, where $\alpha_1, \dots, \alpha_n$ are the roots of f in C. Fix one embedding of K/F into C and let $\tau : F(\alpha_1, \dots, \alpha_n) \to K$ denote its inverse mapping, which is an isomorphism of fields. The correspondence $\sigma \leftrightarrow \tau\sigma$ is a bijection between $\mathrm{Emb}(K/F, C)$ and $\mathrm{Aut}(K/F)$. Thus $|\mathrm{Emb}(K/F, C)| = |\mathrm{Aut}(K/F)|$. Since f is separable we have $|\mathrm{Emb}(K/F, C)| = [K : F]$ by Corollary 6.7. Thus $\mathrm{Aut}(K/F) = [K : F]$.

($2 \Rightarrow 3$) *According to Theorem 8.2* we have $[K : \mathrm{Fix}(\mathrm{Aut}(K/F))] = |\mathrm{Aut}(K/F)|$. By assumption $|\mathrm{Aut}(K/F)| = [K : F]$. This implies that $[K : \mathrm{Fix}(\mathrm{Aut}(K/F))] = [K : F]$. But we have $F \subseteq \mathrm{Fix}(\mathrm{Aut}(K/F)) \subseteq K$, so it follows that $\mathrm{Fix}(\mathrm{Aut}(K/F)) = F$.

($3 \Rightarrow 4$) Let $f(x) \in F[x]$ be irreducible, and suppose that f has a root α in K. We may assume that f is monic. Let $\{\alpha_1, \dots, \alpha_n\}$ be the *distinct* elements of the orbit of α under the group $\mathrm{Aut}(K/F)$. Consider the monic polynomial

$$g(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Clearly g is separable and splits over K. We will complete the proof of this implication by showing that $g = f$.

First observe that any automorphism in $\mathrm{Aut}(K/F)$ permutes the roots of g, and the value of a product of linear polynomials is independent of the order of the factors. Thus the coefficients of g are contained in $\mathrm{Fix}(\mathrm{Aut}(K/F)) = F$. Since α is a root of g and f is the minimal polynomial of α over F, this shows that f divides g. On the other hand, any automorphism in $\mathrm{Aut}(K/F)$ must send roots of f to roots of f. Thus every root of g is a root of f, which implies that g divides f.

($4 \Rightarrow 1$) Let $\beta_1, \ldots, \beta_n$ be a basis for K over F. For each $i = 1, \ldots, n$, let f_i be a minimal polynomial for β_i. Let g be the product of the *distinct* polynomials in the set $\{f_1, \ldots, f_n\}$. Since these are irreducible no two can share a root, and by assumption each of the f_i is separable. Thus g is separable. Also, by assumption, each f_i splits over K, which implies that g splits over K as well. If H is a proper subfield of K then H cannot contain all of $\beta_1, \ldots, \beta_n$. Thus there is at least one root of g which is not contained in H. This shows that K is a splitting field for the separable polynomial g.

This shows that (1) – (4) are equivalent. Now we show that (5) is equivalent to the others. If (5) holds then K is separable over F, so for any algebraically closed extension L of K we have $|\mathrm{Emb}(K/F, L)| = [K : F]$ by Corollary 6.7. Since the image of every embedding of K/F into L is equal to K we have $\mathrm{Emb}(K/F, L) = \mathrm{Aut}(K/F)$. Thus $|\mathrm{Aut}(K/F)| = [K : F]$, which shows that (5) implies (2). On the other hand, (4) implies that K is a separable extension of F and we have already observed in the proof of ($1 \Rightarrow 2$) that if K is a splitting field for a polynomial f with roots $\alpha_1, \ldots, \alpha_n$ then the image of any embedding of K/F into an extension of K must be equal to $F(\alpha_1, \ldots, \alpha_n)$. ☐

Definition 8.4. An finite extension K of a field F is a *normal extension* if it satisfies the equivalent conditions in the statement of Theorem 8.3.

Proposition 8.5. *Suppose that K is a normal extension of a field F and that H is an intermediate field, with $F \subseteq H \subseteq K$. Then K is a normal extension of H.*

Proof. According to Proposition 6.2, K is separable over H. Any embedding of K/H into a field L is also an embedding of K/F into L. But since K is normal over F, any two embeddings of K/F have the same image. Therefore any two embeddings of K/H have the same image. This shows that K is normal over H. ☐

9. The Galois correspondence

Suppose that K is an extension of a field F. If G is a subgroup of $\mathrm{Aut}(K/F)$, we set $\mathcal{F}(G) = \mathrm{Fix}(G)$. If H is an intermediate field, i.e. $F \subseteq H \subseteq K$, then we set $\mathcal{G}(H) = \mathrm{Aut}(K/H)$.

Theorem 9.1. *Suppose that K is a normal extension of a field F. Then $\mathcal{F} \circ \mathcal{G}(H) = H$ for any field H with $F \subseteq H \subseteq K$, and $\mathcal{G} \circ \mathcal{F}(G) = G$ for any subgroup G of $\mathrm{Aut}(K/F)$. In particular, $\mathcal{F}$ and $\mathcal{G}$ are one-to-one correspondences between the set of subfields of K which contain F and the set of subgroups of $\mathrm{Aut}(K/F)$.*

Proof. Proposition 8.5 implies that K is normal over F. Therefore

$$\mathcal{F}(\mathcal{G}(H)) = \mathrm{Fix}(\mathrm{Aut}(K/H)) = H$$

by condition (3) of Theorem 8.3.

On the other hand we have $G \leq \mathcal{G}\mathcal{F}(G) = \mathrm{Aut}(K/\mathrm{Fix}(G))$ since every element of G is an automorphism that fixes $\mathrm{Fix}(G)$. Since K is normal over $\mathrm{Fix}(G)$ by Proposition 8.5, condition (2) of Theorem 8.3 implies that $|\mathcal{G}(\mathcal{F}(G))| = [K : \mathrm{Fix}(G)]$. But Theorem 8.2 implies that $|G| = [K : \mathrm{Fix}(G)]$. Thus $\mathcal{G}(\mathcal{F}(G)) = G$. □

Definition 9.2. Let K be a normal extension of a field F. Suppose that H is a field with $F \subseteq H \subseteq K$, and that G is a subgroup of $\mathrm{Aut}(K/F)$. If $\mathcal{G}(H) = G$ and $\mathcal{F}(G) = H$ then G and H *correspond under the Galois correspondence*.

Theorem 9.3. *Suppose that K is a normal extension of a field F. Let H be a field with $F \subseteq H \subseteq K$ and let G be a subgroup of $\mathrm{Aut}(K/F)$. If G and H correspond under the Galois correspondence then $|G| = [K : H]$, and H is a normal extension of F if and only if G is a normal subgroup of $\mathrm{Aut}(K/F)$.*

Proof. The condition $|G| = [K : H]$ is just condition (2) of Theorem 8.3.

Suppose that $G \trianglelefteq \mathrm{Aut}(K/F)$. To show that H is a normal extension of F we will show that any embedding η of H/F into an algebraically closed extension L of H satisfies $\eta(H) = H$. We can assume that L is an extension of K, by identifying K with the image of some embedding of K/H into L. Now the embedding η extends to an embedding σ of K/F into L. Since K is a normal extension of F, $\sigma(K) = K$, and we may regard σ as an automorphism of K/F. Thus we have an automorphism $\sigma \in \mathrm{Aut}(K/F)$ such that $\eta(H) = \sigma(H)$. But, since G is normal, we have

$$H = \mathrm{Fix}(G) = \mathrm{Fix}(\sigma G \sigma^{-1}) = \sigma(\mathrm{Fix}(G)) = \sigma(H) = \eta(H).$$

This shows that H is a normal extension of F.

Now suppose that H is a normal extension of F. Any automorphism of K/F can be viewed as an embedding of H/F into an algebraic closure of K. Since H is normal over F this implies that $\sigma(H) = H$ for all $\sigma \in \mathrm{Aut}(K/F)$. Thus if $\gamma \in G = \mathrm{Aut}(K/H)$ then $\sigma\gamma\sigma^{-1}$ restricts to the identity on H. This shows that $\sigma\gamma\sigma^{-1} \in G$, so G is a normal subgroup. □

10. Simple extensions

Definition 10.1. Let F be a field and K an extension field of K. If $\alpha \in K - F$ then the field $F(\alpha)$ is a *simple extension* of F. If α is algebraic over F then $F(\alpha)$ is a *simple algebraic extension* of F.

Proposition 10.2. *Let F be a field and let $f(x) \in F[x]$ a monic irreducible polynomial. Let α be a root of f in some extension field of F, and suppose that K is a field with $F \subseteq K \subseteq F(\alpha)$. If $g(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} + x^k \in K[x]$ is the minimal polynomial of α over K, then $K = F(a_0, \ldots, a_{k-1})$.*

Proof. We have $F(a_0, \ldots, a_{k-1}) \subseteq K$ since $g(x) \in K[x]$. Since $g(x)$ is irreducible in $K[x]$ it is also irreducible in $F(a_0, \ldots, a_{k-1})[x]$. Thus

$$[F(\alpha) : F(a_0, \ldots, a_{k-1}] = k = [F(\alpha) : K].$$

If $F(a_0, \ldots, a_{k-1})$ were a proper subfield of K then $[K : F]$ would be a proper divisor of $[F(\alpha) : F(a_0, \ldots, a_{k-1}]$. Thus we must have $K = F(a_0, \ldots, a_{k-1})$. □

We can now give a rather strange looking characterization of simple extensions. The strangeness is due to the fact that the statement does not assume separability, much less normality.

Theorem 10.3. *Suppose that K is a finite extension of a field F. Then $K = F(\alpha)$ for some $\alpha \in K$ if and only if there are only finitely many fields H with $F \subseteq H \subseteq K$.*

Proof. If $F \subseteq H \subseteq F(\alpha)$ then by Proposition 10.2 H is generated by the coefficients of a monic irreducible factor of the minimal polynomial of $f(x)$ over K. But there are only finitely many monic factors of f. In fact, if L is an extension of $F(\alpha)$ such that $f(x)$ splits over L, then any monic factor of $f(x)$ in $K[x]$ must be a product, in $L[x]$ of linear factors of $f(x)$. There are only finitley many such products.

Suppose that there are only finitely many intermediate fields between F and K. If F is finite, then K is also finite. By Exercise 4.2 the multiplicative group of non-zero elements of K is a cyclic group generated by an element $\alpha \in K$. Clearly $K = F(\alpha)$. Thus we may assume that F is an infinite field.

Since K is a finite extension we may write $K = F(\alpha_1, \dots, \alpha_n)$ for some elements $\alpha_1, \dots, \alpha_n \in K$. Let us assume that these elements have been chosen so that n is as small as possible. If $n \geq 2$ then consider the infinitely many elements of K that can be written as $\alpha_1 + t\alpha_2$ for $t \in F$. Each such element determines an intermediate field $F \subseteq F(\alpha_1 + t\alpha_2) \subseteq K$. Since there are only finitely many intermediate fields we must have $F(\alpha_1 + t\alpha_2) = F(\alpha_1 + s\alpha_2)$ for $s \neq t$. According to Lemma 5.1 we then have $F(\alpha_1, \alpha_2) \subseteq F(\alpha_1 + t\alpha_2)$, while clearly $F(\alpha_1 + t\alpha_2) \subseteq F(\alpha_1, \alpha_2)$. Thus $F(\alpha_1 + t\alpha_2) = F(\alpha_1, \alpha_2)$, so $K = F(\alpha_1, \dots, \alpha_n) = F(\alpha_1 + t\alpha_2, \alpha_3, \dots, \alpha_n)$. This is a contradiction, unless $n = 1$. □

Theorem 10.4 (The Primitive Element Theorem)**.** *If K is a finite normal extension of a field F then $K = F(\alpha)$ for some $\alpha \in K$.*

Proof. By Theorem 10.3 we need only show that there are only a finite number of intermediate fields between F and K. Write $K = F(\alpha_1, \dots, \alpha_k)$. For each $i = 1, \dots, n$ let $f_i(x)$ be the minimal polynomial of α_i over F. Let L be the splitting field of the polynomial $f_1(x) \cdots f_k(x)$. Since K embeds in L we may regard L as an extension of K. Since L is a normal extension of F, the intermediate fields between F and K correspond to the subgroups of the finite group $\mathrm{Aut}(L/F)$ which contain the subgroup $\mathrm{Aut}(L/K)$. Thus there are only finitely many intermediate fields. □

11. Cyclotomic polynomials

Let F be a field and let K be an extension of F. Suppose that the polynomial $x^n - 1$ splits over K. The roots of $x^n - 1$ form a finite subgroup of $K^\times$. By Exercise 4.2 this group must be cyclic and, if the polynomial $x^n - 1$ is separable, it will have order n. The polynomial $x^n - 1$ is separable unless $\mathrm{Char}\, F = p \neq 0$ and p divides n. In the case $\mathrm{Char}\, F = n$ the only root of $x^n - 1 = (x - 1)^n$ is 1, so the roots of $x^n - 1$ form a trivial group.

Definition 11.1. A root ζ of $x^n - 1$ in a field F is a *primitive n^{th} root of unity* if n is the smallest positive integer such that $\zeta^n = 1$. In particular, a primitive n^{th} root of unity exists in some extension of F if and only if $x^n - 1$ is separable over F. In this case the roots of $x^n - 1$ form a cyclic group under multiplication, whose generators are exactly the primitive n^{th} roots of unity.

11.2. Suppose that F is a field such that $x^n - 1$ is separable over F. (That is, either $\mathrm{Char}\, F = 0$ or $\mathrm{Char}\, F = p$ where p is a prime that does not divide n.) Let ζ be a primitive n^{th} root of unity in some extension of F. Then $F(\zeta)$ is a splitting field for $x^n - 1$, since all roots of $x^n - 1$ are powers of ζ. If σ is any automorphism of $F(\zeta)/F$ then $\sigma(\zeta) = \zeta^a$ for some integer a which is necessarily relatively prime to n, since $\sigma(\zeta)$ must also be a generator of the (multiplicative) cyclic subgroup consisting of the roots of $x^n - 1$. If $\sigma(\zeta) = \zeta^a$ then σ sends each root of $x^n - 1$ to its a^{th} power, since $\sigma(\zeta^k) = \sigma(\zeta)^k = \zeta^{ak} = (\zeta^k)^a$. Moreover, if σ and τ are two automorphisms of $F(\zeta)/F$ then $\sigma = \tau$ if and only if $\sigma(\zeta) = \tau(\zeta)$. If $\sigma(\zeta) = \zeta^a$ then let $\rho(\sigma)$ be the congruence of $a \pmod{n}$. Notice that ρ is an injective homomorphism from $\mathrm{Aut}(F(\zeta)/F)$ to U_n where U_n denotes the group of units in $\mathbb{Z}/n\mathbb{Z}$ under multiplication. This homomorphism does not depend on the choice of the primitive root ζ since $F(\zeta)$ contains all roots of $x^n - 1$ and since an automorphism of $\mathrm{Aut}(F(\zeta)/F)$ acts by raising all roots of $x^n - 1$ to the same power. Thus we may identify the Galois group of $x^n - 1$ over F with a subgroup $U_n(F)$ of U_n, which depends only on F.

Since $F(\zeta)$ is a splitting field, and hence a normal extension of F, we know that the minimal polynomial $f(x)$ of ζ over F can be written as

$$f(x) = \prod_{a \in U_n(F)} (x - \zeta^a).$$

Thus, $U_n(F)$ can be described as the congruence classes $\pmod{n}$ of integers a such that ζ^a is a root of the minimum polynomial of ζ over F.

The Galois group of any finite extension of $\mathbb{F}_p$ is generated by the Frobenius automorphism, which sends each element to its p^{th} power. Thus if p is a prime which does not divide n then $U_n(\mathbb{F}_p)$ is the subgroup of U_n generated by the congruence class of p.

Definition 11.3. If ζ is a primitive n^{th} root of unity in $\mathbb{C}$, then the polynomial

$$\Phi_n(x) = \prod_{a \in U_n} (x - \zeta^a)$$

is the n^{th} *cyclotomic polynomial*.

Proposition 11.4. *The polynomial $\Phi_n(x)$ is an irreducible polynomial in $\mathbb{Z}[x]$.*

Proof. Let $f(x)$ be the minimal polynomial of ζ over $\mathbb{Q}$. Since $f(x)$ is a monic factor of $x^n - 1$, Gauss' Lemma implies that $f(x) \in \mathbb{Z}[x]$. We will show that $f(x) = \Phi_n(x)$. According to the formula for $f(x)$ given above, this is equivalent to showing that $U_n(\mathbb{Q}) = U_n$. The group U_n is generated by the congruence classes of primes $p < n$ such that p does not divide n. Thus we need only show that $U_n(\mathbb{Q})$ contains every such prime p. That is, we must show that ζ^p is a root of f.

Let p be any prime which does not divide n. Suppose that ζ^p is not a root of $f(x)$. Let $g(x)$ be the minimal polynomial of ζ^p. Then f and g are distinct irreducible factors of $x^n - 1$ and are therefore both in $\mathbb{Z}[x]$. Since ζ is a root of $g(x^p)$, and f is the minimal polynomial of ζ, it follows that $f(x)$ divides $g(x^p)$. Now reduce f and g mod p to obtain polynomials $\bar{f}(x)$ and $\bar{g}(x)$ in $\mathbb{F}_p[x]$. Since $\bar{g}(x^p) = \bar{g}(x)^p$, and $\bar{f}(x)$ divides $\bar{g}(x^p)$, we conclude that $\bar{f}$ divides $\bar{g}$, and hence that $\bar{f}^2$ divides $x^n - 1$. This is a contradiction since $x^n - 1$ is a separable polynomial in $\mathbb{F}_p[x]$. $\square$

Exercise 11.1. Show that the prime factorization of $x^n - 1$ in $\mathbb{Q}[x]$ is

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Exercise 11.2. Compute the prime factorization of $x^8 - 1$ in $\mathbb{F}_2[x]$.

12. Symmetric functions and Discriminants

Let F be a field. Recall that $F[x_1, \ldots, x_n]$ is the ring of polynomials in in the indeterminants $x_1, \ldots, x_n$, while $F(x_1, \ldots, x_n)$ is its quotient field, i.e. the field of rational functions in the indeterminants $x_1, \ldots, x_n$. A polynomial in $F[x_1, \ldots, x_n, t]$ can be regarded as a polynomial in t with coefficients in $F[x_1, \ldots, x_n]$. Thus it makes sense to define elements $s_1, \ldots, s_n \in F[x_1, \ldots, x_n]$ by the condition

$$(t - x_1) \cdots (t - x_n) = t^n - s_n t^{n-1} + \cdots + (-1)^n s_1.$$

The polynomials $s_k(x_1, \ldots, x_n)$ are called the *elmentary symmetric functions* in $x_1, \ldots, x_n$.

For example, we have $s_2(x_1, x_2) = x1x2$ and $s_1(x_1, x_2) = x_1 + x_2$. More generally, if a monic polynomial $f(x)$ in $K[x]$ of degree n has roots $\alpha_1, \ldots, \alpha_n$ in some extension of K, then the coefficient of x^i in f is $(-1)^{n-i} s_i(\alpha_1, \ldots, \alpha_n)$.

Now we regard $s_1, \ldots, s_n$ as elements of the field $F(x_1, \ldots, x_n)$. We can then consider the field extension $F(s_1, \ldots, s_n) \subseteq F(x_1, \ldots, x_n)$.

Proposition 12.1. *The field $F(x_1, \ldots, x_n)$ is a normal extension of $F(s_1, \ldots, s_n)$ with Galois group isomorphic to S_n.*

Definition 12.2. Suppose that K is a splitting field over F for a separable polynomial $f(x) \in F[x]$. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in K. Define

$$\delta(f) = \prod_{0<i<j\leq n} (\alpha_i - \alpha_j).$$

The *discriminant* of f is $D(f) = \delta(f)^2$.

13. Cubic and quartic polynomials

14. Cyclic Galois groups and radical extensions

15. Solvable and nilpotent groups

16. Solvability by radicals

Index of Definitions