MATH 594 - Finite Fields and Galois Theory

AResseges Stery

May 13, 2024

Contents

1 Review of Ring Theory

The Galois Theory originates from the question: Given a polynomial with coefficients in a field (e.g. $\mathbb{Q}$), we want to understand the property of its solutions, and the algebraic structure in which the root lies. This section lays some fundamental notions and results for introducing the whole theory.

Setup the convention. All rings have unit element 1; and all ring homomorphisms map 1 to 1. Inclusion maps, in particular, implies that all subrings of a certain ring must include 1.

> **Remark 1.1.** An immediate result is that finite domains that are not the zero ring are fields.
>
> Recall that a ring R is a domain if and only if zero does not have non-trivial divisors. That is, for all $x, y \in R \setminus \{0\}$, $xy = 0$. For $a \in R$, $a \neq 0$, consider the map
>
> $$\varphi : R \to R \qquad x \mapsto ax$$
>
> Since R is a domain φ maps nonzero elements to nonzero elements, which implies that there exists some x_a s.t. $ax_a = 1$. This gives an inverse of a.

Proposition 1.2. If $f : K \to R$ is a ring homomorphism, and K is a field. Then $R \neq \{0\}$ implies that f is injective.

Proof. Recall that the kernel of a particular ring homomorphism is an ideal. Denote $I = \ker(f) \subseteq K$. Suppose that $a \in I$ s.t. a is nonzero. Then $a^{-1} \in I$ which gives $I = (1) = K \implies f(I) = 0$. But as we requre $f(1) = 1_R \implies 1_R = 0_R$, i.e. $R = \{0\}$ which is a contradiction. □

> **Corollary 1.3.** In particular, ring homomorphisms between fields (field extensions) $K \to L$ are injective. Not all fields have extensions (ring homomorphisms) between them.

A class of extensions of which we are particularly interested in, is the extension which gives polynomial a root. $f \in K[x]$ may not have a root; and by extending it $K[x] \hookrightarrow L[x]$ we may consider roots of $f \in L[x]$ which may have a root.

Notation. A field extension $k \hookrightarrow K$ is also denoted as K/k. These two notations will be used interchangeably.

Proposition 1.4. Let k be a field, and $R = k[X]$. Let $f \in R \setminus \{0\}$. Then the followings are equivalent:

1) f is irreducible.
2) (f) is a prime ideal.
3) (f) is a maximal ideal.

Proof. Prove the implications cyclically:

- *3) $\implies$ 2).* It is a general fact that maximal ideals are prime. Prove the contrapositive: suppose that an ideal $(f) \subset R$ is not prime, then there exists $a, b \in R$ s.t. $ab \in (f)$ and neither a and b are in (f). Then $(f) \subset (a) \subset R$ which implies that (f) is not maximal.
- *2) $\implies$ 1).* (f) being a prime ideal in R implies that in particular $(f) \neq R$, i.e. f is not invertible. Suppose that there exists g, h not invertible s.t. $f = gh$. Without loss of generality, assume that $g \in (f)$. Then there exists some $u \in R$ s.t. $g = fu$. Multiply on the right by h gives $f = gh = fuh$ which implies that h is invertible, giving a contradiction.

- *3) $\implies$ 1).* f being irreducible implies that f is not invertible, i.e. $(f) \neq R$. Suppose that there exists some maximal ideal J s.t. $(f) \subset J \subset R$. Then since maximal ideals are in particular prime, $J = (g)$ for some $g \in R$. But then this implies that $f = gu$ giving that u is invertible, and therefore $(f) = J$, which is a contradiction.

□

Recall that two elements f, g are relative prime if for all $p \in R$ s.t. $p \mid f, p \mid g$, p is invertible. Then we have the following result similar to the case for integer divisibility:

Proposition 1.5. Let k be a field, and $R = k[x]$. For $f, g, h \in R$ s.t. $f \mid gh$, if f and g are relative prime, then $f \mid h$.

Proof. Since k is a field, $k[x]$ is a PID (as every element in the coefficient is invertible, for a, b relative prime $(a, b) = (1) = k[x]$). Consider $I = (f, g) \subseteq R$. Since I is principal, $I = (p)$ for some $p \in k[x]$. Therefore $p \mid f, p \mid g$, which implies that p is invertible. Then $I = R$. This gives that there exists $A, B \in R$ s.t. $Af + Bg = 1$. Multiplying h on the right gives $Afh + Bgh = h$. Since f divides LHS, $f \mid h$. □

Proposition 1.6. Let k be a field, and $R = k[x]$. If $f \in R \setminus \{0\}$, and denoting $d = \deg f$, then there exists field extensions $k \hookrightarrow L$ and $a_1, \ldots, a_d \in L, c \in k$ s.t. $f = c(x - a_1) \cdots (x - a_d)$ in $L[x]$.

Proof. The key step is to show that if f is irreducible in R, then there exists a field extension $k \hookrightarrow k'$ s.t. f has a root in k'.

Consider $k' = k[x]/(f)$. Since f is irreducible, (f) is a maximal ideal in R, and therefore k' is a field. Since elements in k are of degree 0 in $k[x]$. Considering $k \longrightarrow k[x] \longrightarrow k' := k[x]/(f)$ gives the injective ring homomorphism (field extension). Let $a = \overline{x} \in k'$. Then $f(a) = \overline{f(x)} = 0$, which implies that a is a root of f.

Proceed the rest of the proof by induction:

- $d = 0$. This is the trivial case.
- $d = 1$. Then $f = c(x - a)$ for some $c, a \in k$.
- $d \geq 2$. Apply the above steps iteratively. Then there exists some $a \in k'$ s.t. $(x-a) \mid f$, i.e. in $k'[x]$ we have the decomposition $f = (x - a)g$ for some $g \in k'[x]$ with $\deg g = \deg f - 1$. Applying the inductive hypothesis (the results holds in lower degrees) gives the full decomposition in $L := k'$.

□

Notation. Denote the image of the map $(k[y] \to k, y \mapsto a)$ by $k[a]$. This is the smallest k-algebra containing a.

Proposition 1.7. Let k be a field, and $R = k[x]$. Let $f \in R \setminus \{0\}$ be irreducible. Suppose that we have the field extension $k \hookrightarrow K$, and $a \in K$ is a root of f. Then $k[a] \simeq k[x]/(f)$. In particular, $k[a]$ is a field.

Proof. Consider the ring homomorphism $\varphi : k[y] \to K$ s.t. $\varphi(y) = a$. Then by the First Isomorphism Theorem, we have $k[a] = \operatorname{im} \varphi \simeq k[x]/\ker \varphi \simeq k[x]/(f)$ since $f(a) = 0$. □

Notice that every field extension $k \hookrightarrow K$ is a k-algebra morphism (ring homomorphisms that are k-linear). Since k is a field, this gives K a k-vector space structure.

Definition 1.8 (Degree). The **degree** of the field extension $k \hookrightarrow K$, denoted $[K : k]$, is $\dim_k K \in \mathbb{Z}_{\geq 0}$ or infinite.

Definition 1.9 (Finite). A field extension is **finite** if the degree of it is finite.

Remark 1.10. If $f \in k[x]$ is irreducible, and $K = k[x]/(f)$, then $[K : k] = \deg f$. More generally, if $g \in k[x]$ is a nonzero polynomial, then $\dim_k(k[x]/(g)) = \deg g$.

This can be seen via applying the division algorithm (since $K[x]$ is an Euclidean Domain. This can be seen via computing the division). Then for all $P \in k[x]$, there exists unique $Q, R \in k[x]$ s.t. $P = gQ + R$, with $\deg R < \deg g$. Then since $\overline{P} = \overline{R}$ in $k[x]/(g)$, $\{\bar{1}, \bar{x}, \ldots, \overline{x^{\deg g - 1}}\}$ gives a basis of $k[x]/(g)$ over k.

2 Multiplicity of Root

This section provides tools for describing the zeros of a polynomial, and how they in general can look like. The proposition below says that any polynomial can be factored into two parts, with the first part having roots in the field; and the second part requires extension of the field to decompose completely.

Definition 2.1 (Multiplicity). Let $f \in k[x]$ be a nonzero polynomial for k a field, and $a \in R$ a root of f, Then a has **multiplicity** m if $(x - a)^m \mid f$, but $(x - a)^{m+1} \nmid f$.

Proposition 2.2. If $f \in R \setminus \{0\}$, and $a_1, \ldots, a_r \in k$ are pairwise distinct roots of f s.t. a_i has multiplicity m_i. Then we have the decomposition of f:

$$f = \prod_{i=1}^{r} (x - a_i)^{m_i} g, \qquad g \in R, g(a_i) \neq 0 \text{ for all } i$$

In particular, $\sum_i m_i \leq \deg f$.

Proof. Apply induction on r:

- *Base case.* Then m_1 is the maximal integer satisfying the condition that $(x - a_1)^{m_1} \mid f$. Then define g be such that $f = (x - a_1)^{m_1} g$.
- *Inductive step.* For $r \geq 2$, denote f_1 be the polynomial s.t. $f = (x - a_1)^{m_1} f_1$. Notice that for all i s.t. $2 \leq i \leq r$, we have $(x - a_i)^{m_i} \mid f$. Then since $(x - a_i)$ and $(x - a_1)$ are relative prime (they are both irreducible) by Proposition 1.5 we have $(x - a_i)^{m_i} \mid f_1$. Then applying inductive hypothesis gives the desired decomposition of f.

□

3 Characteristic of a Field

Recall that in the first section we mentioned that there does not necessarily exist ring homomorphisms between arbitrary fields. This, as we will see in the following, implies some constraints on the structure that a field can have.

Let S be an integral domain. Let $\varphi : \mathbb{Z} \to S$ s.t. $n \mapsto n \cdot 1_S$. This is the unique ring homomorphism between $\mathbb{Z}$ and S due to the constraint the 1 should be mapped to 1. Since S is a domain, and $\mathbb{Z}$ is a PID, $\ker \varphi = (d)$ for d prime or zero. Then either

1) $\ker \varphi = \{0\}$; or

2) $\ker \varphi = p\mathbb{Z}$ for some p prime.

In case 1), if we suppose further that $S = k$ which is a field, then for all $n \in \mathbb{Z}$ $\varphi(n)$ is invertible. By the universal property of the quotient ring, this induces a ring homomorphism (which is also a field extension) $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q} \hookrightarrow S$.

In case 2), we have an injective ring homomorphism $\mathbb{Z}/p\mathbb{Z} \hookrightarrow S$ for some p prime. Defining $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, S becomes an $\mathbb{F}_p$-algebra by the φ above.

Definition 3.1 (Characteristic). For a field k, the **characteristic** of k is

$$\mathrm{char}(k) = \begin{cases} p, & \text{if } \mathbb{F}_p \hookrightarrow k \text{ (case 1)} \\ 0, & \text{if } \mathbb{Q} \hookrightarrow k \text{ (case 2)} \end{cases}$$

Remark 3.2. If S is an $\mathbb{F}_p$-algebra (case 2), the map $F : S \to S$, $u \mapsto u^p$ is the Frobenius homomorphism. Check that this is indeed a ring homomorphism:

- $F(uv) = F(u)F(v)$. Clear as field is commutative: $(uv)^p = u^p v^p$.
- $F(u+v) = F(u) + F(v)$. Compute:

$$(u+v)^p = u^p + v^p + \underbrace{\sum_{i=1}^{p-1} \binom{p}{i} u^{p-i} v^i}_{\text{divisible by } p}$$

  where the last term vanishes, as $\mathbb{F}_p \hookrightarrow S$ should map 0 to 0; and $\bar{p} = \bar{0} \in \mathbb{F}_p$.

4 Algebraic Extensions

The field extensions originating solely from "including the roots of polynomials" are the nice ones and deserve a better name. The discussions formalizes the concept of "algebraic closure" in elementary discussions of polynomials.

Proposition 4.1. If $k \hookrightarrow K \hookrightarrow L$ is a field extension, then $[L : k] = [L : K][K : k]$.

Proof. First consider the cases where one of the degrees is infinite:

- If $[K : k]$ is infinite, then $[L : k]$ is infinite as $K \subseteq L$ is a K-vector subspace of L.
- If $[L : K]$ is infinite, then there exists an infinite set of elements which are linearly independent over K, which are also linearly independent over k since $k \subseteq K$.

Now consider the case where both $[L : K]$ and $[K : k]$ are finite. Denote $m = [L : K]$ and $n = [K : k]$. Denote $\{a_1, \dots, a_m\}$ be a basis of L over K, and $\{b_1, \dots, b_n\}$ be a basis of K over k. Notice that $\{a_i b_j \mid 1 \le i \le m, 1 \le j \le n\}$ gives a basis for L over k, as for all $u \in L$, there exists $\lambda_i \in K$, and thus $\mu_{ij} \in k$ s.t.

$$u = \sum_{i=1}^{n} \lambda_i b_i = \sum_{i,j} \mu_{ij} a_j b_i, \qquad \text{for } \lambda_i = \sum_j \mu_{ij} a_j \mu_{ij}$$

which is a decomposition. They are further linearly independent, as for $u = 0$, since b_is give a basis, $\lambda_i = 0$ for all i, and therefore $\mu_{ij} = 0$ for all i and j. □

Notation. Let $k \hookrightarrow K$ be a field extension, and $A \subseteq K$ a subset. Then we denote

$$k(A) := \bigcap_{A \subseteq k'} \{k' \mid k \hookrightarrow k' \hookrightarrow K \text{ extension}\}$$

which is the smallest field sub-extension of k inside K containing A.

Remark 4.2. It is worth mentioning that this is different from $k[A]$ which is the smallest k-*subalgebra* containing A:

- They are related via $k(A) = \mathrm{Frac}(k[A])$. They are equal in some "nice" extensions (see Remark 4.9 below).

  By definition we have $k[A] \subseteq k(A)$, as $k[A]$ is only required to be a k-algebra instead of a field extension of k (as field extending k can be seen as k-vector spaces, which are in particular k-algebras). By the universal property of fraction fields, we have $\mathrm{Frac}(k[A]) \subseteq k(A)$, as ring homomorphisms between fields are injective, and by definition for all $f \in k[A]$, f has an inverse in $k(A)$. Further since $A \subseteq \mathrm{Frac}(k[A])$ (also by definition, we have $k(A) = \mathrm{Frac}k[A]$).

- Considering multiple elements, we can extend the previous notation, by considering for $A = \{a_1, \dots, a_n\}$, then $k[A] = \mathrm{im}\, \varphi$ for

  $$\varphi : k[x_1, \dots, x_n] \to K, \qquad x_i \mapsto a_i$$

Definition 4.3 (Finite Generated). A field extension K/k is **finitely generated** if there exists $a_1, \dots, a_n \in K$ s.t. $k(a_1, \dots, a_n) = K$.

Remark 4.4. If a field extension K/k is finite, then it is also finitely generated, as K/k being finite implies that there exists some finite basis of K over k; and picking one gives the elements that "finitely generates" K. However, the converse is not true: consider $k \hookrightarrow k(x) = \mathrm{Frac}(k[x])$ is finitely generated (by x) but is not finite (we have the infinite set $\{x^i \mid i \in \mathbb{Z}\}$ whose elements are linearly independent over k)

Definition 4.5 (Algebraic; Transcendental). Let $k \hookrightarrow K$ be a field extension. An element $a \in K$ is **algebraic over** k if there exists $f \in k[x] \setminus \{0\}$ s.t. $f(a) = 0$ in $K[x]$. Otherwise a is **transcendental**. An extension K/k is **algebraic** if for all $a \in K$, it is algebraic over k.

Remark 4.6. Consider the field extensions $k \hookrightarrow K \hookrightarrow L$. Then if $a \in L$ is algebraic over k, then a is also algebraic over K, as a algebraic over k implies that there exists $f \in k[x]$ s.t. $f(a) = 0$; and by definition we also have $f \in K[x]$.

Remark 4.7. Given a field extension $k \hookrightarrow K$, and $a \in K$. Then a is algebraic if and only if the $\varphi : k[x] \to k, x \mapsto a$ has a non-trivial kernel. This is the direct translation of having a polynomial f with a as its root. Then $\ker \varphi$ is a prime ideal.

To prove this, it suffices to show that $k[x]/(\ker \varphi)$ is a domain. This is indeed the case, as $k[x]$ is a domain: for all $g, h \in k[x]$, $g(a) \neq 0$ and $h(a) \neq 0$ implies that $gh(a) \neq 0$, i.e. $gh \notin \ker \varphi$ ($gh \neq \bar{0}$ in $k[x]/(\ker \varphi)$). Therefore, there exists some f s.t. $\ker \varphi = (f)$.

Definition 4.8 (Minimal Polynomial). $f \in k[x]$ is the **minimal polynomial** of $a \in K$ if for $\varphi : k[x] \to K$, $x \mapsto a$, $\ker \varphi = (f)$. This is well-defined by the above Remark (Remark 4.7).

Remark 4.9. For a being algebraic, f is a maximal ideal (by the fact that $k[x]/(\ker \varphi)$ is a domain). Then $k[a] = k[x]/(\ker \varphi)$ is a field. This gives $k[a] = k(a)$.

Remark 4.10. Given field extension K/k, if $a \in K$ is transcendental over k, then $k[a] \simeq k[x]$, as since there is no polynomial with root a implies that $k[a]$ can be seen as injecting a formal variable to the field $k[x]$. This further implies $k(a) \simeq k(x)$ (as $k(a) \simeq \mathrm{Frac}(k[a])$; and same for x).

Example 4.11. Suppose that $d \in \mathbb{Z}$ is not a square, and let $a = \sqrt{d}$. Consider the field extension $\mathbb{Q} \to \mathbb{C}$.

Since a is not in $\mathbb{Q}$, a cannot be a root of degree 1 polynomials, i.e. the minimal polynomial of a must be of degree at least 2; and we have a as a root of $x^2 - d = 0$, the minimal polynomial of a over k is $x^2 - d = 0$, which also implies that a is algebraic over $\mathbb{Q}$.

Therefore, $\mathbb{Q}(\sqrt{d})$ can be seen as a $\mathbb{Q}$-vector space, which has a basis $\{1, \sqrt{Q}\}$, i.e. $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$. In particular we have $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{d}) = 2$ as $\deg f = 2$, resulting from Remark 1.10.

Proposition 4.12. Every finite extension K/k is algebraic.

Proof. Denote $[K : k] = n$ which is finite. Regarding K as a k-vector space, for all $a \in K$ the set of elements $\{1, a, \ldots, a^n\}$ are linearly dependent (as there are $(n+1)$ of them). That is, there exists $c_0, \ldots, c_n \in k$ s.t. $c_0 + c_1 a + \cdots + c_n a^n = 0$; and $f = c_0 + c_1 x + \cdots + c_n x^n \in k[x] \setminus \{0\}$. This gives a polynomial $f \in k[x]$ s.t. $f(a) = 0$, i.e. a is algebraic. Since $a \in K$ can be taken arbitrarily, we have K/k being algebraic. □

Proposition 4.13. Let $k \hookrightarrow K$ be a field extension, and $a_1, \ldots, a_n \in K$ are algebraic over k. Then $k[a_1, \ldots, a_n] = k(a_1, \ldots, a_n)$; and $k(a_1, \ldots, a_n)$ is a finite extension over k.

Proof. Remark 4.9 gives the case for $n = 1$, $k[a] = k(a)$, and Remark 1.10 (using minimal polynomial) gives that the extension is finite.

For $n \geq 2$, repeat the argument with the induction hypothesis. First by definition we have $k[a_1, \ldots, a_n] = (k[a_1, \ldots, a_{n-1}])[a_n]$; and the same holds for the field extension version (replace brackets with parentheses). Further finite extensions are transitive, by Proposition 4.1. Suppose now that $k' = k[a_1, \ldots, a_{n-1}] = k(a_1, \ldots, a_{n-1})$ is a finite extension over k. Then $k[a_1, \ldots, a_n] = k'[a_n] = k'(a_n) = k(a_1, \ldots, a_n)$ is finite over k'; and by hypothesis we know $k'[a_n]$ is finite over k since k' is. □

Corollary 4.14. Finitely generated algebraic field extensions are finite.

Proposition 4.15. If $k \hookrightarrow K \hookrightarrow L$ are both algebraic field extensions, then so is $k \hookrightarrow L$.

Proof. Use the above two propositions. Let $a \in L$. Since L/K is algebraic, there exists $f \in K[x] \setminus \{0\}$ s.t. $f(a) = 0$. Let $f = c_0 + c_1 x + \cdots + c_n x^n$, and $k' = k(c_0, \ldots, c_n)$. Since all $c_0, \ldots, c_n \in K$ are algebraic over k, Proposition 4.13 implies that k' is a finite extension over k. Further since a is algebraic over k', the extension $k' \hookrightarrow k'(a)$ is also finite. Proposition 4.12 implies that the extension $k \hookrightarrow k'(a)$ is algebraic. That is, a is algebraic over k.

Since this holds for all $a \in L$, the extension L/k is algebraic. □

Remark 4.16. Notice that the converse of the statement is also true. If $k \hookrightarrow L$ is algebraic, then for every element $a \in L$ there exists some $f_a \in k[x]$ s.t. $f_a(a) = 0$. But given extension $k \hookrightarrow K \hookrightarrow L$, $k \subseteq K$, which implies f_a is also in $K[x]$; and therefore L/K is algebraic

Proposition 4.17. If $k \hookrightarrow K$ is a field extension, then $k' = \{a \in K \mid a \text{ algebraic over } k\}$ is a subfield of K containing k,

Proof. To prove this we need to check:

- $k \subseteq k'$. This is clear from the construction of the field.
- k' is closed under additive and multiplicative inverse.

  $a \in k'$ implies $-a \in k'$ as $-a$ is the root of a polynomial via considering the minimal polynomial and inverting the corresponding coefficients. $a \in k' \setminus \{0\}$ implies $a^{-1} \in k' \setminus \{0\}$ since $k[a] = k(a)$ as $k(a)$ is finitely generated, and therefore finite and algebraic. $k(a)$ is a field, implying that $a^{-1} \in k(a)$.
- k' is closed under addition and multiplication. That is, for all $a, b \in k'$, $a + b \in k'$ and $ab \in k'$.

  Consider the field $k(a, b)$. Since both a and b are algebraic over k, $k(a, b)/k$ is finite by Proposition 4.13; and by Proposition 4.12 the extension is algebraic. By definition $k(a, b) \subseteq k'$; and is the smallest field containing both a and b; and therefore both $a + b$ and ab are in k'.

□

Definition 4.18 (Algebraic Closure)**.** For a field k with field extension $k \hookrightarrow K$, the field $k' = \{a \in K \mid a \text{ algebraic over } k\}$ is the **algebraic closure** of k in K. By the above Proposition 4.17, this is indeed a field.

Definition 4.19 (Algebraically Closed)**.** A field k is **algebraically closed** if every nonzero polynomial over k has a root in k.

Remark 4.20. By induction, if k is algebraically closed and f is a nonzero polynomial in $k[x]$ with degree n¡ then there exists $a_1, \ldots, a_n \in k$, $c \in k^*$ s.t. $f = c(x - a_1) \cdots (x - a_k)$. That is, every irreducible polynomial in an algebraically closed field has degree 1.

Notation. For a field k, the set of invertible (nonzero) elements in it are often denoted as k^* or $k^\times$.

Proposition 4.21. A field k is algebraically closed if and only if for all field extensions $k \hookrightarrow K$, for all $a \in K \setminus k$, a is transcendental over k.

Proof. Prove implication in two directions:

$\Rightarrow$: Suppose that k is algebraically closed, and $a \in K \setminus k$ algebraic over k. Then by definition there exists an irreducible polynomial $f \in k[x]$ s.t. $f(a) = 0$. Since k is algebraically closed, the irreducible polynomials are of degree 1, i.e. $\deg f = 1$. Then $a \in k$, which is a contradiction.

$\Leftarrow$: Suppose that for all $a \in K \setminus k$, a is transcendental. Proceed to prove that k is algebraically closed by showing that every irreducible polynomial has a root.

Consider $f \in k[x] \setminus \{0\}$. Consider $K = k[x]/(f)$. Then since $f(\bar{x}) = 0$, $\bar{x}$ is algebraic over k. But since all elements in $K \setminus k$ are transcendental, $\bar{x} \in k$. Then in K we have $\bar{x} - a = 0$, for some $a \in k$. Then $f(x) = x - a$ in $K[x]$ which has a root a; and as this holds for all f, k is algebraically closed.

□

In summary, a field k being algebraically closed is equivalent to the following conditions:

1) For all field extensions $k \hookrightarrow K$, either $k \simeq K$, or the extension is not algebraic.
2) For all $f \in k[x] \setminus \{0\}$, f factors as a product of polynomials of degree 1.
3) Every irreducible $f \in k[x] \setminus \{0\}$ has a root in k.

Recall that we have the algebraic closure in a specific field. The following theorem seeks to construct such closure without any ambient structure:

Theorem 4.22. Given any field k, there exists an algebraic extension $k \hookrightarrow \bar{k}$ s.t. $\bar{k}$ is algebraically closed. Such an extension is an algebraic closure of k.

Parenthesis 4.23 (Direct Limit (of rings)). To provide the construction of an algebraic closure, the main step is to iteratively include the roots of the some irreducible polynomials; and we need to ensure that this process terminates. That is, there exists a field containing all the intermediate fields on which we conducted the extension. This parenthesis formalizes this idea.

Definition 4.24 (Directed Set). $(I, \leq)$ is a **directed set** if for all $i, j \in I$ there exists $k \in I$ s.t. $i \leq k$ and $j \leq k$.

Definition 4.25 (Direct System). Given a directed set I, a **direct system** $(R_i)_{i \in I}$ is a family of rings R_i satisfying:

- For all $i \leq j$ in I, there exists a ring homomorphism $\varphi_{ij} : R_i \to R_j$; and $\varphi_{ii} = \mathrm{Id}_{R_i}$.
- For all $i \leq j \leq k$ in I, the ring homomorphisms above satisfy $\varphi_{ik} = \varphi_{jk} \circ \varphi_{ij}$.

Definition 4.26 (Direct Limit). Given a direct system $(R_i)_{i\in I}$, the **direct limit** of the system, denoted $R = \varinjlim R_i$, together with a family of ring homomorphisms $f_i : R_i \to R$ s.t.

- $f_j \circ \varphi_{ij} = f_i$.
- The pair $(R, (f_i)_{i\in I})$ is universal with this property, i.e. every ring homomorphism from R_i for all i factors uniquely through R. That is, for any ring T and family of ring homomorphisms $g_i : R_i \to T$ s.t. $g_j \circ \varphi_{ij} = g_i$ (the g_is are compatible w.r.t. the system), there exists a unique ring homomorphism $g : R \to T$ s.t. $g \circ f_i = g_i$ for all i.

The direct limit exists, by considering the class of elements that are closed along the morphisms of R_is: define $R := \left(\bigsqcup_{i\in I} R_i\right) / \sim$, where the equivalence relation $\sim$ is given by $R_i \ni x_i \sim \varphi_{ij}(x_i)$. The operations are given by for $a_i \in R_i$ and $b_j \in R_j$, finding k s.t. $i \le k$ and $j \le k$ (which exists as I is a directed set), and define:

$$a_i + b_j := \varphi_{ik}(a_i) + \varphi_{jk}(b_j) \in R_k, \qquad a_i b_j := \varphi_{ik}(a_i) \cdot \varphi_{jk}(b_j) \in R_k$$

Existence of inverse, and distributivity are guaranteed by the ring structure of R_j. Further see that this is well-defined, as for $k' \neq k$ that we have picked s.t. $i \le k'$ and $j \le k'$, since the set is directed there exists ℓ s.t. $k \le \ell$ and $k' \le \ell$. Now use the equivalence relation with $\varphi_{k\ell}$ and $\varphi_{k'\ell}$; and the fact that $\sim$ is an equivalence relation and is therefore transitive.

Further the direct limit of a direct system is unique up to isomorphism. Suppose we have two direct limits R and R', there exists $g : R \to R'$ and $g' : R' \to R$, by the universal property of the direct limit s.t. $g \circ f_i = f'_i$, $g' \circ f'_i = f_i$. This implies that $g \circ g' = \mathrm{Id}_{R'}$, and $g' \circ g = \mathrm{Id}_R$ by the symmetric argument. This gives the isomorphism.

The last thing we need to notice is that if all R_is are fields, then R is a field, as in the definition of the operation having multiplicative inverse in R_k induces the multiplicative inverse in R.

Now we can use the above tools to describe the polynomial with variables indexed by a (possibly infinite) set I. Given a commutative ring R, a set I, the polynomial ring $R[x_i \mid i \in I]$ is defined as follows:

For $J \subset I$ finite subset, denote $R_J := R[x_i \mid i \in J]$. Define $\mathcal{P} := \{\text{finite subsets of } I\}$, ordered by inclusion. This is a directed set, as for all $M, N \in \mathcal{P}$, we have $M \subseteq I$ and $N \subseteq I$ by definition.

For $J_1 \subseteq J_2$ in $\mathcal{P}$, we have a morphism of R-algebras $\varphi_{J_1 J_2} : R_{J_1} \to R_{J_2}$, $x_i \mapsto x_i$ (embeddings). This gives a direct system of R-algebras; and we can define $R[x_i \mid i \in I] := \varinjlim(R_J)_{J\in P}$. Notice:

- All $\varphi_{J_1 J_2}$ are injective (as they are embeddings), and therefore the map $R_J \to R[x_i \mid i \in I]$ is also injective.
- Observe that we have $\bigcup_{J\in\mathcal{P}} R_J$ is a direct limit of the system $(R_J)_{J\in\mathcal{P}}$; and since the direct limit is unique up to isomorphisms for a particular directed system, we have $R[x_i \mid i \in I] = \bigcup_{J\in\mathcal{P}} R_J$.

Now prove the theorem:

Proof of Theorem 4.22. As we have mentioned, the idea of the proof is to construct a direct system of fields, where each φ (which is a field extension here) includes the roots of irreducible polynomials in the base field; then taking the direct limit of the system gives the desired algebraic closure.

The first step is to construct a field extension $k \hookrightarrow k_1$ s.t. for all $f \in k[x]$ irreducible, there exists $a \in k_1$ s.t. $f(a) = 0$. Define $A = \{f \in k[x] \mid f \text{ irreducible}\}$. Define $R = k[y_f \mid f \in A]$ and $\underline{a} = (f(y_f) \mid f \in A)$ where y_f are formal variables indexed by polynomials in A; and the parenthesis in $\underline{a}$ implies that this is an ideal generated by such elements.

Claim that $\underline{a} \neq R$. First observe that by definition $\underline{a} \subseteq R$, as in particular we have $f \in k[y_f] \subseteq k[y_f \mid f \in A] =: R$. Suppose that $\underline{a} = R$. Then the condition is translated to:

$$\exists r \in \mathbb{Z}_{>0},\ f_1, \dots, f_n \in A,\ g_1, \dots, g_n \in R, \qquad \sum_{i=1}^{r} \underbrace{g_i}_{\in R} \underbrace{f_i(y_{f_i})}_{\in \underline{a}} = 1 \tag{$*$}$$

as the ideal being equal to the whole ring is the same as the ideal containing 1. By Proposition 1.7, for all i there exists field extension $k \hookrightarrow k_i$ s.t. there exists $a_i \in k_i$ satisfying $f_i(a_i) = 0$. Since there finitely many (exactly r) polynomials, we can do this iteratively and get a field extension $k \hookrightarrow K$ s.t. there exists field extensions $k_i \hookrightarrow K$ for all i.

Let $J \subseteq A$ be the finite subset containing all the f_is, and also containing all polynomials g s.t. y_g appears in some $g_i \in k$. Define $\varphi : k[y_g \mid g \in J] \hookrightarrow K$. $y_{f_i} \mapsto a_i$ for all i, and $y_g \mapsto \varepsilon \in K$ which is some value we do not care about. Recall that a_is are defined s.t. $f_i(a_i) = 0$. This is a k-algebra morphism.

Now apply φ to Eq. ($*$). Since φ is k-linear, we have

$$0 = \sum_{i=1}^{r} \varphi(g_i) f_i(a_i) = \varphi(1) = 1$$

which is a contradiction, as for a field we require $0 \neq 1$. Therefore $\underline{a} \neq R$. Further since $\underline{a}$ is an ideal in R, there exists a maximal ideal M in R s.t. $\underline{a} \subseteq R$. Define $k' = R/M$ which is not trivial since $\underline{a} \neq R$. Denote $k_1 := \{a \in k' \mid a \text{ algebraic over } k\}$. By Proposition 4.17 this is a subfield of k', and by definition is algebraic over k. Now consider $f \in k[x]$ irreducible, and $\overline{y_f} \in k' = R/M$ a formal variable. By definition of algebraic closure, $f(\overline{y_f}) = 0$ in $\bar{k}$; and since $f(y_f) \in \underline{a} \subseteq M$, $\overline{f(y_f)} = f(\overline{y_f}) = 0 \in R/M$, which implies that $\overline{y_f} \in k_1$. Since $k' = R/M$ with R extending elements in the form of y_f, every element in k' is in the same as $\overline{y_f}$ for some $f \in A$; and by the previous argument we know $k \hookrightarrow k'$ is algebraic. That is, every $f \in k[x]$ irreducible has a root in k_1.

Now repeat the process with k replace by k_1. Conducting induction gives that for all $f \in k_i[x]$, there exists $a \in k_{i+1}$, $f(a) = 0$ in $k_{i+1}[x]$. This gives algebraic extensions

$$k \hookrightarrow k_1 \hookrightarrow k_2 \hookrightarrow \cdots$$

Now take $\bar{k} := \varinjlim k_i$. This is a field by Parenthesis 4.23 satisfying $k \hookrightarrow k_i \hookrightarrow \bar{k}$, and by the following remark $\bar{j} = \bigcup_{i \geq 1} k_i$. Check:

- *$\bar{k}$ is algebraic over k.* This results from the fact that each of the intermediate extension is algebraic; and the result follows from Proposition 4.15.
- *$\bar{k}$ is algebraically closed.* For all $f \in \bar{k}[x]$, there exists i s.t. $f \in k_i[x]$. Then f has a root in k_{i+1} which can be extended to K by universal property of direct limit.

□

Remark 4.27. If the field k is infinite, the algebraic closure $\bar{k}$ is of the same cardinality as k.

To address the uniqueness of $\bar{k}$, we prove the following theorem that is more general:

Theorem 4.28. Given two field extensions $k \hookrightarrow K$ and $k \hookrightarrow L$ s.t. K/k is algebraic, and L is algebraically closed. Then there is a morphism of k-extensions $K \hookrightarrow L$, where a morphism of k-extensions is a morphism of k-algebras which is the identity map when restrict to k.

To prove the theorem we need Zorn's Lemma:

Lemma 4.29 (Zorn). Given a nonempty ordered set $(A, \leq)$ s.t. every chain in A has an upper bound in A. Then a has a maximal element. The terminologies are:

- A chain is a totally ordered subset.
- An upper bound for $B \subseteq A$ is an element $a \in A$ s.t. for all $b \in B, b \leq a$.
- A maximal element in A is some $a \in A$ s.t. for all a' s.t. $a \leq a'$, we have $a' = a$.

Proof of Theorem 4.28. Consider the set $A = \{(k', \varphi)\}$ where k' is a subfield of K for which there exists extensions $k \hookrightarrow k' \hookrightarrow K$; and for $i : k \to k'$, $j : k \to L$ we have $\varphi \circ i = j$. Define the partial order on A be such that $(K', \varphi) \leq (K'', \psi)$ if and only if $K' \subseteq K$, and $\psi|_{k'} = \varphi$.

Now apply Zorn. Check the followings:

- A is non empty. In particular, $(k, j) \in A$.
- Suppose that $B = \{(K_i, \varphi_i) \mid i \in I\}$ is a chain (totally ordered subset) in A, Then B has a maximal element (which also serves as an upper bound) (K, φ) given by $K = \bigcup_{i \in I} K_i$ and φ be such that $\varphi|_{K_i} = \varphi_i$. Such φ exists as B is totally ordered, i.e. for any subset of B the maximal element gives the corresponding φ.

Then Zorn's Lemma gives that there exists a maximal element $(K', \varphi) \in A$. Then either:

- $K' = K$. This gives the desired result.
- $K' \neq K$. We seek to find a contradiction. Since $K' \subseteq K$, there exists $a \in K \setminus K'$. Since K/k is algebraic by hypothesis, by Remark 4.16, K/K' is also algebraic. Let $f \in K'[x]$ be the minimal polynomial of a over K'. Try to extend on a:

$$K' \hookrightarrow K'[a] \simeq K'(a) \simeq K'[x]/(f)$$

where $K'[a] = K'(a)$ since a is algebraic over k'. Since L is algebraically closed, f (considering it in $L[x]$) has a root $b \in L$. Then there exists a unique K'-algebra morphism $\varphi' : K'(a) \to L$, $a \mapsto b$, which is indeed a K'-algebra morphism as any $g \in K[x]$ s.t. $g(a) = 0$ satisfies $f \mid g$, which has b also as a root. But then $(K'(a), \varphi')$ satisfies the condition, which contradicts with the maximality of (K', φ).

Therefore $K' = K$ and we have the desired result. □

Corollary 4.30. The algebraic closure of a given field k is unique up to isomorphism.

Suppose that we have field extensions $k \hookrightarrow K$ and $k \hookrightarrow L$, with both K and L algebraically closed. Then applying the above theorem twice gives field extensions $K \hookrightarrow L$ and $L \hookrightarrow K$, which are both injective by Proposition 1.2. This gives the desired isomorphism.

Notation. Since the algebraic closures of a specific field k are isomorphic, we can simply refer to it as *the* algebraic closure, and denote it with $\bar{k}$.

Remark 4.31. We have the following immediate results:

1) If $k \hookrightarrow K$ is algebraic, and $K \hookrightarrow \overline{K}$ algebraic closure, then $k \hookrightarrow \overline{K}$ is also an algebraic closure (by considering $f \in k[x]$ as elements of $K[x]$).

2) If we have $k \hookrightarrow K$ a field extension, and K is algebraically closed. Then for $k' := \{a \in K \mid a \text{ algebraic over } k\}$ we have k'/k an algebraic closure. This is clearly algebraic by definition; and it is closed as if $f \in k'[x] \setminus \{0\}$, there exists $a \in K$ s.t. $f(a) = 0$ as K is algebraically closed. Then a is algebraic over $k \implies k' \hookrightarrow k'(a)$ finite $\implies k' \hookrightarrow k'(a)$ algebraic $\implies k \hookrightarrow k' \hookrightarrow k'(a)$ algebraic. But this gives the fact that a is algebraic over k, and since $a \in K$ by definition $a \in k'$.

Notice that we cannot use the same trick in the proof for Theorem 4.22 as in that case the extensions $k \hookrightarrow k_1$ is not necessarily algebraic.

Now we can use the above results to classify finite fields:

Let K be a finite field. Since $\mathbb{Z} \to K$ cannot be injective, $\operatorname{char}(K) = p$ for some prime p. This gives a field extension $\mathbb{F}_p \hookrightarrow K$; and since $e = [K : \mathbb{F}_p]$ is finite (since K is finite), $|K| = p^e$ for some e. Denote $\overline{K}$ to be the algebraic closure of K. By Remark 4.31 this is also the algebraic closure of $\mathbb{F}_p$.

Claim 4.32. $K = \{u \in \overline{K} \mid u^{p^e} = u\}$. This gives the existence of finite fields with order p^e.

Proof. Notice that $(K^\times, \cdot)$ is a finite group with $(p^e - 1)$ elements. Therefore, for all $u \in L$, $u^{p^e - 1} = 1$, which implies that $u^{p^e} = u$ i.e. $K \subseteq$ RHS. Now consider the polynomial $x^{p^e} - x$ in $\overline{K}[x]$, which has p^e roots since $\overline{K}$ is algebraically closed. $|K| = p^e$ gives the desired equality. □

Proposition 4.33. If K_1 and K_2 are both fields with p^e elements, then $K_1 \simeq K_2$. Without ambiguity we denote such fields as $\mathbb{F}_{p^e}$.

Proof. Consider the extensions:

$$\begin{array}{ccc} \mathbb{F}_p & \hookrightarrow & K_1 \\ \downarrow & & \downarrow \varphi \\ K_2 & \hookrightarrow & \overline{K_2} \end{array}$$

This existence of φ is guaranteed by Theorem 4.28. Since φ is a ring homomorphism between fields, it is injective; and therefore $|\varphi(K_1)| = |K_1| = p^e \implies \varphi(K_1) = \{i \in \overline{K_2} \mid u^{p^e} = u\}$. But this then coincides with K_2. □

Example 4.34. There exists a ring homomorphism $\mathbb{F}_{p^e} \to \mathbb{F}_{p^f}$ if and only if $e \mid f$.

Proof. Verify both implications:

$\Rightarrow$: Since we have the field extension $\mathbb{F}_{p^e} \hookrightarrow \mathbb{F}_{p^f}$, we can view $\mathbb{F}_{p^f}$ as a $\mathbb{F}_{p^e}$-vector space. As further we have two fields being finite, $\left|\mathbb{F}_{p^f}\right| = (|\mathbb{F}_{p^e}|)^{\dim_{\mathbb{F}_{p^e}} \mathbb{F}_{p^f}}$. In particular this implies that $e \mid f$.

$\Leftarrow$: By Claim 4.32 we know that the elements in the field $\mathbb{F}_{p^f}$ are those in the set $\{u \in \overline{\mathbb{F}_{p^f}} \mid u^{p^f} = u\}$. Now Consider the roots of the polynomial $f = x^{p^f} - x$ in $\overline{\mathbb{F}_{p^f}}$. Since $\mathbb{F}_{p^f}$ embeds naturally into its algebraic closure, the image is exactly the roots of f. Since $e \mid f$, there exists n s.t. $f = ne$. Notice then that f factors as follows:

$$f = x^{p^f} - x = \left(x^{p^e} - x\right)\left(\sum_{i=1}^{n-1} p^{i(p^e-1)}\right)$$

which implies that elements satisfying the relation $u^{p^e} = u$ in particular also satisfy $u^{p^f} = u$; and by Claim 4.32 these give the elements in field $\mathbb{F}_{p^e}$. This gives the field extension $\mathbb{F}_{p^e} \hookrightarrow \mathbb{F}_{p^f} \hookrightarrow \overline{\mathbb{F}_{p^f}}$ (and also by the uniqueness of algebraic closure (Corollary 4.30) we have $\overline{\mathbb{F}_{p^e}} = \overline{\mathbb{F}_{p^f}}$).

□

Example 4.35. Inside the algebraic closure of $\mathbb{F}_p$, $\overline{\mathbb{F}_p}$, for all $e \geq 1$ we have a unique copy of $\mathbb{F}_{p^e}$; and $\overline{\mathbb{F}_p} = \bigcup_{e \geq 1} \mathbb{F}_{p^e}$.

Proof. Proceed to verify the inclusion in both directions:

$\subseteq$ For any element $u \in \overline{\mathbb{F}_p}$, consider its minimal polynomial over $\mathbb{F}_p$. Let $f_u \in \mathbb{F}_p[x]$ be the polynomial of u. Then $u \in \mathbb{F}_p(u) \simeq \mathbb{F}_p[x]/(f_u)$. By Remark 1.10 we have $|\mathbb{F}_p(u)| = p^{\deg f} \implies u \in \mathbb{F}_{p^{\deg f}} \subseteq \bigcup_{e \geq 1} \mathbb{F}_{p^e}$.

$\supseteq$ By Example 4.34 we have the embedding of $\mathbb{F}_{p^e}$ to its algebraic closure; and also such closures can be identified by the uniqueness of algebraic closure and viewing $\mathbb{F}_{p^n}$ as elements satisfying relation $u^{p^n} = u$ by Claim 4.32.

□

5 The Splitting Field of a Polynomial

Definition 5.1 (Splitting Field). Let k be a field, and $f \in k[x] \setminus \{0\}$. A **splitting field** of f is a field extension $k \hookrightarrow K$ s.t.

1) f factors in $K[x]$ as a product of degree-1 polynomials.

2) If there exists K' s.t. $k \subseteq K' \subseteq K$ which also satisfies 1), then $K' = K$,

Equivalently, for a splitting field of f, denoted K, we can write f in $K[x]$ as $f = c(x-a_1)\cdots(x-a_n)$ with $c, a_1, \ldots, a_n \in K$; and $K = k(a_1, \ldots, a_n)$.

Example 5.2. $\mathbb{C}$ is the splitting field of x^2+1. $\mathbb{Q}(\sqrt{2})$ is the splitting field of x^2-2.

From what we had proved previously (Corollary 4.30), we know that algebraic closure is unique up to isomorphism, so we would expect the splitting field to be unique up to isomorphisms as well. The followings use (which will also be the case for most proofs regarding existence of extensions) the algebraic closure to construct such extensions.

Theorem 5.3. If $f \in k[x] \setminus \{0\}$, then

1. There exists a splitting field $k \hookrightarrow K$ of f.
2. If we have $k \hookrightarrow K$, $k \hookrightarrow K'$ splitting fields of f, then $K \simeq K'$ as k-extensions.

Remark 5.4. If K is the splitting field of $f \in k[x]$, then K/k is a finite extension, as in particular K is generated (as a k-vector space) by finitely many algebraic elements over k, namely the roots of f. By Proposition 4.13 the extension is then finite.

Proof of Theorem 5.3. Prove the two statements respectively:

1) Consider $k \hookrightarrow \bar{k}$ the algebraic closure of k. Then there exists $c, a_1, \dots, a_n \in \bar{k}$ s.t. $f = c(x-a_1)\cdots(x-a_n)$. Then $K = k(a_1, \dots, a_n)$ is the splitting field of f, by definition.

2) Let $k \hookrightarrow K$ and $k \hookrightarrow K'$ be the splitting fields of f. Let $K' \hookrightarrow \overline{K'}$ be the algebraic closure. By the remark above, K/k is algebraic. Since $\overline{K'}$ is algebraically closed, by Theorem 4.28 there exists $\varphi : K \to \overline{K'}$ s.t. $\varphi|_k = \mathrm{Id}_k$. Since K and K' are splitting fields of f over k, we can write $f = c(x-a_1)\cdots(x-a_n)$ in $K[x]$, and $f = c'(x-a_1')\cdots(x-a_n')$ in $K'[x]$. This gives the similar expression of the fields as in the remark:

$$K = k(a_1, \dots, a_n), \qquad K' = k(a_1', \dots, a_n')$$

Consider the ring homomorphism $K[x] \hookrightarrow K'[x] \subseteq \overline{K'}[x]$ induced by φ, we have

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

since $f \in k[x]$ and φ as a morphism between k-extensions is the identity map when restricted to k. Therefore φ permutes a_is, which gives $\varphi(K) \subseteq K'$ and $\varphi(K') \subseteq K$, i.e. $\varphi(K) = K'$, and φ is bijection and thus a ring isomorphism.

□

6 Separable Extensions

Definition 6.1 (Separable Extension)**.** Let $k \hookrightarrow K$ be an algebraic field extension. An element $a \in K$ is **separable over** k if its minimal polynomial $f \in k[x]$ satisfies any of the following conditions:

1) a is not a multiple root of f.
2) $f' \neq 0$.

3) Either $\mathrm{char}(k) = 0$, or $\mathrm{char}(k) = p > 0$, and $f \notin k[x^p]$.

Such a polynomial f is a **separable polynomial**. A field extension $k \hookrightarrow K$ is **separable** if the minimal polynomial of any element in K is separable.

Proposition 6.2. The three conditions in Definition 6.1 for separability over a field are equivalent.

Proof. Verify the following implications:

- *2) $\Longrightarrow$ 1).* Prove the contrapositive. Suppose that a is a root of f with multiplicity at least 2. Then we have $(x-a)^2 \mid f \implies (x-a) \mid f'$, i.e. $f'(a) = 0$. Since f is minimal, $f' \mid f$, and yet we require $\deg f' = \deg f$, which implies that $f = 0$.
- *1) $\Longrightarrow$ 2).* Prove the contrapositive by reversing the logic above. f minimal implies $f'(a) = 0$ if and only if $f \mid f'$. But $f'(a) = 0 \implies (x-a)^2 \mid f$, i.e. a is a multiple root of f.
- *3) $\Longrightarrow$ 2).* If $\mathrm{char}(k) = 0$, then $f' = 0$ if and only if f is constant, which cannot be a minimal polynomial. If $\mathrm{char}(k) = p$, then if $f' = 0$ either f is constant (which cannot be the case) or every term of f' vanishes because of characteristic-p, i.e. $f \in k[x^p]$.
- *2) $\Longrightarrow$ 3).* Reverse the logic above and verify by the same computation.

□

Remark 6.3. Notice that the condition 2) $f' \neq 0$ does not depend on whether f splits into degree-1 polynomials. Therefore, if $f \in k[x]$ is separable, then f cannot have any multiple roots in any algebraic closure of k.

Definition 6.4 (Perfect Field)**.** A field k is **perfect** if every extension $k \hookrightarrow K$ is separable.

Proposition 6.5. A field k is perfect if and only if $\mathrm{char}(k) = 0$, or $\mathrm{char}(k) = p$ with $k = k^p$, i.e. the map $\varphi : k \to k, x \mapsto x^p$ is an isomorphism.

Proof. For the case where k is characteristic-0, any minimal polynomial f must be of degree at least 1, giving $f' \neq 0$ which satisfies condition 2).

Now consider the case where $\mathrm{char}k = p$. Show the following two implications:

- *If there exists $a \in k \setminus k^p$, then k is not perfect.* Let $k \hookrightarrow \bar{k}$ be an algebraic closure, and let $b \in \bar{k}$ be a root of $f = x^p - a$. Claim that f is irreducible in k (which implies that b is not separable over k as it is a multiple root). In $k[x]$, $f = x^p - a = x^p - b^p = (x-b)^p$ since $\mathrm{char}k = p$. Therefore, if $f = gh$ in $k[x]$ with $\deg g > 0$ and $\deg h > 0$, g must taken the form of $g = c(x-b)^i$ for $1 \leq i \leq p-1$. But then consider the coefficient of x, which gives $cib \in k$. Since $c, i \neq 0$ in k, $b \in k$, which is a contradiction.
- *If $k = k^p$, then k is perfect.* Suppose that we have the algebraic extension $k \hookrightarrow K$. Choose $u \in K$ arbitrarily, with minimal polynomial f. If u is not separable over k, then by definition $f \in k[x^p]$, i.e. we can write f as

$$f = \sum_{i=0}^{n} a_i x^{p^i} = \sum_{i=0}^{n} b_i^p x^{p^i} = \left(\sum_{i=1}^{n} b_i x^i \right)^p$$

where the first equality results from $k = k^p$, and the second equality results from $\mathrm{char} k = p$. But this contradicts with the irreducibility of f.

□

Example 6.6. The followings give some examples of separability of extensions:

1. Every field of characteristic 0 is perfect by the proposition above.
2. Every algebraically closed field k is perfect, as the only algebraic extension from k is $k \hookrightarrow k$.
3. Every finite field $\mathbb{F}_{p^e}$ is perfect, as Claim 4.32 gives that $u \in \mathbb{F}_{p^e} \implies u^{p^e} = u$, i.e. $\left(u^{p^{e-1}}\right)^p = u$; and using the proposition above gives the desired result.
4. Fields in the form of $k(x)$ where $\mathrm{char} k = p > 0$ is not perfect. Suppose that $x \in (k(x))^p$, then $x = \left(\frac{f}{g}\right)^p$ for some $f, g \in K[x]$, i.e. $xg^p = f^p$. Counting the degree of the polynomial on both sides, we have $1 \equiv 0 \pmod p$, which is a contradiction.

Proposition 6.7. If we have field extensions $k \hookrightarrow k_1 \hookrightarrow k_2$ s.t. the extension $k \hookrightarrow k_2$ is separable, then both $k \hookrightarrow k_1$ and $k_1 \hookrightarrow k_2$ are separable.

Proof. $a \in k_1$ can be considered as an element in k_2; and since $k \hookrightarrow k_2$ is separable, a is not a multiple root of its minimal polynomial over k, which implies that $k \hookrightarrow k_1$ is separable.

For the second result, consider $b \in k_2$. Let g be its minimal polynomial over k, and h be its minimal polynomial over k_1. h being minimal implies that $h \mid g$. Since $k \hookrightarrow k_2$ is separable, b is not a multiple root of g, and therefore is not a multiple root of h. Since this holds for all $b \in k_2$, the extension $k_1 \hookrightarrow k_2$ is also separable. □

The converse of the proposition above also holds, but we will prove this later.

THe following results characterize the "nice" feature of a field extension being separable:

Definition 6.8 (Primitive Element)**.** Given a field extension E/F, $\alpha \in F$ is a **primitive element** if $E = F(\alpha)$.

Definition 6.9 (Simple Extension)**.** A field extension E/F is simple if there exists a primitive element for the extension.

Theorem 6.10. Every finite separable extension is simple.

Proof. Since K/k is finite, there exists a basis of K seen as a k-vector field. In particular there exists $a_1, \ldots, a_n \in K$ s.t. $K = k(a_1, \ldots, a_n)$. Perform induction on n:

- $n = 1$. Clear.
- $n \geq 2$. It suffices to show the case for $n = 2$, as since the extension is finite, recursively apply the result for $n = 2$ will give the general result. Suppose that $K = k(a, b)$ for $a, b \in K$.

  If k is a finite field, then K is also finite, which implies that $K^\times$ is a cyclic group. Let $c \in K^\times$ be a generator of $K^\times$. Then we have $K = k(c)$.

Now suppose that k is finite. We seek to prove a stronger result: if $c_\lambda = a\lambda + b$ for $\lambda \in k$, then c_λ is a primitive element for finitely many λ. Fix $\lambda \in k$. Suppose that c_λ is not primitive, i.e. we have $k(c_\lambda) \subseteq k(a,b)$ a proper extension. Then we must have $a \notin k(c_\lambda)$ (as otherwise we get $k(c_\lambda) \ni c_\lambda - a\lambda = b$). Let $f, g \in k(c_\lambda)[x]$ be the minimal polynomials of a and b over $k(c_\lambda)$. Then in the algebraic closure $K \hookrightarrow \overline{K}$, f and g factors as

$$f = (x-a_1)\cdots(x-a_n), \qquad g = (x-b_1)\cdots(x-b_m)$$

Without loss of generality assume that $a = a_1$ and $b = b_1$. Since $a \notin k(c_\lambda)$, $n \geq 2$. Now consider the extensions $k \hookrightarrow k(c_\lambda) \hookrightarrow k(a,b)$. Since $k \hookrightarrow k(a,b)$ is separable, $k \hookrightarrow k(c_\lambda)$ is also separable, which by definition implies that all the a_is are distinct. Now consider $\varphi : k(c_\lambda)(a_1) \xrightarrow{\sim} k(c_\lambda)(a_2)$ which sends $a_1 \mapsto a_2$. We then have the commutative diagram:

$$\begin{array}{ccccc} k(c_\lambda) & \hookrightarrow & k(c_\lambda)(a_1) & \hookrightarrow & \bar{k} \\ & \searrow & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \psi} \\ & & k(c_\lambda)(a_2) & \hookrightarrow & \bar{k} \end{array}$$

This induces an isomorphism $\psi : \bar{k} \to \bar{k}$ via specifying $\psi(b) = \psi(b_1) = b_i$ for some i. Since ψ should fix $k(c_[\lambda])$, we require

$$a_2\lambda + b_i = \psi(a\lambda + b) = \psi(c_\lambda) = a\lambda + b \implies \lambda = \frac{b_i - b}{a - a_2}$$

Such lambda exists since $a \neq a_2$ by the previous result that all a_is are distinct; and there are only finitely many of them as there are finitely many distinct b_is.

□

7 Normal Extensions

Definition 7.1 (Normal Extension). An algebraic extension $K \hookrightarrow L$ is a **normal extension** if it satisfies one of the following three conditions:

1) For every $f \in K[x]$ irreducible, if f has a root in L, then f factors as degree-1 polynomials in $L[x]$.

2) There is a (possibly infinite) family of polynomials $(f_i)_{i\in I}$ in $K[x]$ s.t. L is the splitting field of this family. That is, all f_i factors as a product of degree-1 polynomials in $L[x]$, and there is no L' with $K \subset L' \subset L$ which satisfies the same property.

3) Given an algebraic closure $L \hookrightarrow \bar{L}$, any ring homomorphism $\sigma : L \hookrightarrow \bar{L}$ satisfying $\sigma|_K = \mathrm{Id}_K$ satisfies $\sigma(L) \subseteq L$.

Proposition 7.2. The three conditions in the Definition 7.1 for normal extensions are equivalent.

Proof. Verify the following implications:

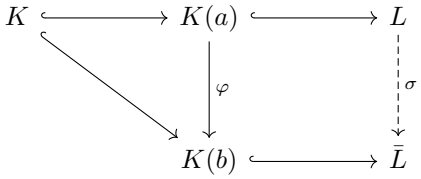
- *1) $\implies$ 2).* Choose a family of elements $(a_i)_{i\in I}$ s.t. $L = K(a_i \mid i \in I)$. Since the extension L/K is algebraic, for all i, a_i has

a minimal polynomial f_i. Since f_i has a root a_i in L, it factors as

$$f_i = (x - a_{i1}) \cdots (x - a_{in_i}), \qquad \text{where } a_{i1} = a_i,\ a_{ij} \in L$$

Then we can write $L = K(a_{ij} \mid i \in I, 1 \leq j \leq n_i)$, which exactly implies that L is the splitting field of $(f_i)_{i \in I}$.

- *2) $\implies$ 3).* If L is the splitting field of $(f_i)_{i \in I}$, then $f_i = (x - a_{i1}) \cdots (x - a_{in_i})$ with $a_{i1} = a_i$, and $a_{ij} \in L$ for all i, j. Since σ fixes elements in K,
$$f_i = \sigma(f_i) = \sigma(c_1)(x - \sigma(a_{i1})) \cdots (x - \sigma(a_{in_i}))$$
Then $\sigma(a_{ij}) \in \{a_{i1}, \ldots, a_{in_i}\} \subseteq L$ for all j. Since 2) gives that $L = K(a_{ij} \mid i \in I, 1 \leq j \leq n_i)$, we know $\sigma(L) \subseteq L$ as σ fixes K and is thus uniquely determined by its action on a_{ij}s.

- *3) $\implies$ 1).* Let $f \in K[x]$ be irreducible, and has a root $a \in L$. Let $L \hookrightarrow \bar{L}$ be an algebraic closure. Prove by contradiction: suppose that f has a root $b \in \bar{L} \setminus L$. Consider the map $\varphi : K(a) \to K(b)$ fixing K and mapping a to b. Since $K(a) \hookrightarrow L$ is algebraic, and $\bar{L}$ is algebraically closed, by Theorem 4.28 there exists a unique $\sigma : L \hookrightarrow \bar{L}$ extending φ, i.e. we have the following commutative diagram:


But then $\sigma(a) = b \notin L$ which gives a contradiction.

□

Remark 7.3. From the proof, if the extension we have $K \hookrightarrow L$ is a finite normal extension, then there exists finitely many $f_1, \ldots, f_r \in K[x]$ s.t. L is the splitting field of $(f_1, \ldots, f_r)$ then equivalently L is the splitting field of $f = \prod_{i=1}^{r} f_i$.

Example 7.4. The following gives some examples of normal extensions:

1. The algebraic closure $K \hookrightarrow \bar{K}$ is normal as by definition any ring homomorphism σ has the property $\sigma(K) \subseteq K$.
2. If $K \hookrightarrow L$ is a degree-2 extension, then L/K is normal. If $a \in L \setminus K$, and f is the minimal polynomial of a, then by Remark 1.10 $\deg f = 2$, i.e. $f = (x - a)(x - b) \in K[x]$. Then since $a \in L$, $b \in L$ as $a + b \in K \subseteq L$. But this implies that L is the splitting field of f and therefore L/K is normal.
3. The extension $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt[3]{2})$ is normal as $\mathbb{Q}(\sqrt[3]{2})$ does not contain all the roots of $x^3 - 2$.

Proposition 7.5. Let $K \hookrightarrow L \hookrightarrow L'$ be algebraic extensions, and L'/K is normal. Then there exists normal sub-extension $L \hookrightarrow \tilde{L} \hookrightarrow L'$ s.t. $\tilde{L}/K$ is normal. This is the normal closure of L over K.

Proof. Write $L = K(a_i \mid i \in I)$. Denote $f_i \in K[x]$ as the minimal polynomial of a_i. Since L'/K is normal, we can factor $f_i = \sigma(f_i) = \sigma(c_1)(x - \sigma(a_{i1})) \cdots (x - \sigma(a_{in_i}))$ with $a_i = a_{i1}$, and $a_{ij} \in L'$ for all j. If we have $L \subseteq \tilde{L} \subseteq L'$ where $\tilde{L}/L$ is normal, then $a_{ij} \in \tilde{L}$, which implies that $K(a_{ij} \mid i \in I, 1 \leq j \leq n_i) \subseteq \tilde{L}$. Since $K \hookrightarrow K(a_{ij} \mid i \in I, 1 \leq j \leq n_i)$ is the splitting field of the family of polynomials $(f_i)_{i \in I}$, $\tilde{L}/K$ is normal. □

Remark 7.6. If we have $K \hookrightarrow L \hookrightarrow L_1'$ and $K \hookrightarrow L \hookrightarrow L_2'$ algebraic extensions s.t. L_1'/L and L_2'/L are normal, then the corresponding normal closures of L in L_1' and L_2' are isomorphic as k-extensions.

Proposition 7.7. If $K \hookrightarrow L \hookrightarrow L'$ are algebraic extensions, and L'/K is normal, then L'/L is normal.

Proof. Suppose that $f \in L[x]$ is irreducible, and has a root $a \in L'$, then f is a minimal polynomial of a over L. Let $g \in K[x]$ be the minimal polynomial of a over K. By definition $g(a) = 0$, which implies that $f \mid g$ in $L[x]$. Since L'/K is normal, g factors as a product of degree-1 polynomials in $L'[x]$, which implies that f also factors as a product of degree-1 polynomials in $L'[x]$, which is exactly the definition of L'/L being normal. □

8 Galois Extensions

Definition 8.1 (Galois Group)**.** Let $K \hookrightarrow L$ be an algebraic extension. The **Galois Group** of L/K is

$$G(L/K) := \{\sigma \in \mathrm{Aut}(L) \mid \sigma|_K = \mathrm{Id}_K\}$$

with the group operation defined as composition.

Definition 8.2 (Galois Extension)**.** A field extension is **Galois** if it is both normal and separable.

Theorem 8.3. For $K \hookrightarrow L$ a finite Galois extension, $|G(L/K)| = [L : K]$.

Proof. Since L/K is finite and separable, by Theorem 6.10 there exists a primitive $a \in L$ s.t. $L = K(a)$. Let f be the minimal polynomial of a over K. By Remark 1.10 we know $\deg f = [L : K]$.

Now consider the algebraic closure $K \hookrightarrow L \hookrightarrow \bar{L}$. THen f factors as $f = (x - a_1) \cdots (x - a_n)$ with $a_1 = a$, $a_i \in \bar{L}$ for all i, and $n = [L : K]$. Since L/K is normal, $a_i \in L$ for all i as $a \in L$; and since L/K is separable, all a_is are distinct. Further as $f \in K[x]$, for all $\sigma \in G(L/K)$, $f = \sigma(f) = (x - \sigma(a_1)) \cdots (x - \sigma(a_n))$. Then $\sigma(a_i) \in \{a_1, \ldots, a_n\}$ for all i.

Define $\varphi : G(L/K) \to \{a_1, \ldots, a_n\}$, $\sigma \mapsto \sigma(a_1)$. Check:

- *φ is injective.* Since $L = K(a)$, two automorphisms in $G(L/K)$ agreeing on a must be identical as by definition they must fix K.
- *φ is surjective.* For all i, since f is irreducible over K, we have $K(a) \simeq K[x]/(f) \simeq K(a_i)$ as K-algebras. Extend this to $\sigma : L \to L$, i.e. making the following diagram commute:

$$\begin{array}{ccc} K(a) & \xrightarrow{\sim} & K(a_i) \\ \| & & \cap| \\ L & \xrightarrow{\sigma} & L \end{array}$$

  Notice that σ must be surhective, as

$$[K(a) : K] = [L : K] = [K(a_i) : K] \leq [\sigma(L) : K]$$

which implies that $L \subseteq \sigma(L)$ and therefore σ is an automorphism, i.e. is in $G(L/K)$. This gives a pre-image and thus implies that φ is surjective. Since $\{a_1, \ldots, a_n\}$ is a finite set, $|G(L/K)| = |\{a_1, \ldots, a_n\}| = n$.

□

Remark 8.4. With the same notation as in the proof, we have a group homomorphism $G(L/K) \to S_n \simeq S_{\{a_1,\ldots,a_n\}}$, $\sigma \mapsto (a_i \mapsto \sigma(a_i))$. Since it is both injective and surjective as given by the proof, the induced action of $G(L/K)$ on $\{a_1, \ldots, a_n\}$ is transitive.

Corollary 8.5. Automorphisms in $G(L/K)$ permutes the roots of minimal polynomials of elements in L over K.

Example 8.6. The followings give some examples of Galois extensions and the corresponding Galois Group:

1. $\mathbb{R} \hookrightarrow \mathbb{C}$ is a Galois extension of degree 2. It is normal as $\mathbb{C}$ is the splitting field of $x^2 + 1$, and it is separable as $\mathbb{R}$ is characteristic-0. $G(\mathbb{C}/\mathbb{R}) = \{\mathrm{Id}, \sigma\}$ where σ is the complex conjugation (corresponding to S_2).
2. For $d \in \mathbb{Z}_{\geq 0}$ not a perfect square, $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{d})$ is a Galois extension of degree 2. It is normal as $\mathbb{Q}(\sqrt{d})$ is the splitting field of $x^2 - d$, and it is separable as $\mathbb{Q}$ is characteristic-0. $G(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{\mathrm{Id}, \sigma\}$ where $\sigma : (a + b\sqrt{d}) \mapsto (a - b\sqrt{d})$.
3. $\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^e}$ is a Galois extension with degree e. It is normal as $\mathbb{F}_{p^e}$ is the splitting field of $x^{p^e} - x$; and it is separable as $\mathbb{F}_{p^n}$ is perfect for all n. The Galois group is then $G(\mathbb{F}_{p^e}/\mathbb{F}_p) = \langle\sigma\rangle$ where σ is the Frobenius endomorphism: $x \mapsto x^p$, with $\sigma^e = \mathrm{Id}$ and $|\langle\sigma\rangle| = e$.

   A sidenote is that using this perspective it is clearer that there exists an embedding $\mathbb{F}_{p^e} \hookrightarrow \mathbb{F}_{p^f}$ if and only if $e \mid f$, as this is equivalent to saying that $\sigma^f = \mathrm{Id}$.
4. The extension $\mathbb{Q} \overset{\deg 3}{\hookrightarrow} \mathbb{Q}(\sqrt[3]{2}) \overset{\deg 2}{\hookrightarrow} \mathbb{Q}(\sqrt[3]{2}, \omega)$ where ω is the 3-rd root of unity, is Galois, as it is the splitting field of $x^3 - 2$ (normal) and $\mathbb{Q}$ is perfect (separable). Since $G(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ is not cyclic, $G(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \simeq S_3$ by cardinality.

9 Algebraic Independence & Transcendence Degree*

The introduction of transcendental degree seeks to give an invariant that measures how far the an extension $k \hookrightarrow K$ is from being algebraic. We would denote this as $\mathrm{trdeg}(K/k)$ and give a formal definition later. But we would desire the following properties from it:

1) $\mathrm{trdeg}\, K/k = 0$ if the extension $k \hookrightarrow K$ is algebraic.

2) If $k \hookrightarrow K = k(x_1, \ldots, x_n)$ where $x_1, \ldots, x_n$ are formal (not algebraic), then $\mathrm{trdeg}(K/k) = n$.

3) Given extensions $k \hookrightarrow K \hookrightarrow L$, $\mathrm{trdeg}(L/k) = \mathrm{trdeg}(K/k) + \mathrm{trdeg}\, L/K$.

Definition 9.1 (Algebraic Independence). Given a field extension $k \hookrightarrow K$, a subset $A \subset K$ is **algebraically independent** (over k) if for all n for every $a_1, \ldots, a_n \in A$ distinct, and every $f \in k[x_1, \ldots, x_n]$, $f \neq 0$ implies $f(a_1, \ldots, a_n) \neq 0$. Otherwise we say that A os **algebraic dependent**.

Remark 9.2. We have the following immediate results:

1) For $A = \{a\}$, i.e. containing only one element, then A is algebraically independent if and only if a is not algebraic over k.
2) By definition, A is algebraically independent if and only if for all $B \subseteq A$ finite, B is algebraically independent.
3) Given $a_1, \dots, a_n \in k$, they being algebraically independent if and only if for $\varphi : k[x_1, \dots, x_n] \to k$, $x_i \mapsto a_i$ as a k-algebra homomorphism satisfies $\ker \varphi = \{0\}$, i.e. $k(a_1, \dots, a_n) \simeq k(x_1, \dots, x_n)$.

Example 9.3. Take $R = k[x, y]/(x^2 + y^2 - 1)$, consider $k \hookrightarrow R \hookrightarrow \mathrm{Frac}(R)$, $\bar{x}$ and $\bar{y}$ are algebraically dependent, as we have the relation $(\bar{x})^2 + (\bar{y})^2 = 1$.

Proposition 9.4. Given a field extension $k \hookrightarrow K$, let A be a set, and $B = A \sqcup \{b\}$ inside field K. Then B is algebraically independent over k if and only if A is algebraically independent over k, and b is not algebraic over $k(A)$.

Proof. By definition if B is algebraically independent, then A must be algebraically independent. For b not algebraic over the $k(A)$ prove the contrapositive: suppose that B is algebraic over $k(A)$, then there exists $0 \neq P = c_0 + c_1 y + \cdots + c_d y^d \in k(A)[y]$ s.t. $P(b) = 0$. Since $c_i \in k(A)$, we can write $c_i = \frac{f_i(a_1, \dots, a_n)}{g_i(a_1, \dots, a_n)}$ for $f_i, g_i \in k[x_1, \dots, x_n]$ and $a_i \in A$. $P(b) = 0$ implies that $\sum_{i=0}^{d} f_i(x_1, \dots, x_n) b^i = 0$. But notice that $P \neq 0$, and P can be viewed as a polynomial in $\{a_1, \dots, a_n, b\}$, which implies that A is not algebraically independent.

The other direction is clear by definition. □

Proposition 9.5. Every algebraically independent subset $A \subseteq K$ over k is contained in a maximal such subset.

Proof. Apply Zorn's Lemma. Show that the set $\mathcal{B} = \{B \subseteq K \mid A \subseteq B, B \text{ algebrically independent over } k\}$ with order of inclusion satisfies the hypotheses in Zorn's Lemma:

- $\mathcal{B}$ is nonempty. In particular, it contains A.
- If $(B_i)_{i \in I}$ is a chain in $\mathcal{B}$, it is bounded above by $\overline{B} = \bigcup_{i \in I} B_i \in B$. It is indeed algebraically independent as every finite subset of $\overline{B}$ is contained in some B_i since every two such B_is are comparable (as a chain is totally ordered).

□

Proposition 9.6. A subset $A \subseteq L$ is a maximal algebraically independent subset over k of K if and only if A is algebraically independent, and $k(A) \hookrightarrow K$ is an algebraic extension.

Proof. By definition, if A is algebraically independent, then it is maximal if and only if for all $b \in K \setminus A$, b is algebraic over $k(A)$ (otherwise by Proposition 9.4 we can adjoin an element to this set while keeping its algebraic independence). This is exactly saying that $k(A) \hookrightarrow K$ is algebraic. □

Definition 9.7 (Transcendental Basis). Given a field extension K/k, a **transcendental basis** of K/k is a maximal algebraically independent subset of K over k.

Definition 9.8 (Transcendental Degree). Given a field extension K/k, the **transcendental degree**, denoted $\mathrm{trdeg}(K/k)$ is the number of elements of a transcendental basis. It is in $\mathbb{Z}_{\geq 0} \cup \infty$.

We are using the similar nomenclature as for vector spaces, so we would expect similar properties for being "independent" or "a basis":

Theorem 9.9. If given K/k is a field extension, and $a_1, \ldots, a_n \in K$ s.t. $k(a_1, \ldots, a_n) \hookrightarrow K$ is algebraic (i.e. this is a maximal algebraically independent set), then for all $\{b_1, \ldots, b_m\}$ algebraically independent over k, $m \leq n$.

Proof. After reordering the elements, we may assume that $a_i = b_i$ for all $1 \leq i \leq r$. If $r = m$ then this is exactly hat we need.

Now suppose that $r < m$. It is enough to show that there exists $i > r$ s.t. the extension $k(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n, b_{r+1}) \hookrightarrow K$ is algebraic. If that is the case, then after finitely many steps we will get the set b_ns (as we can identify $a_1, \ldots, a_r, a_{r+1}$ with the corresponding elements in b and apply the argument recursively). This then implies that $r = m$.

Since b_{r+1} is algebraic over $k(a_1, \ldots, a_n)$, there exists nonzero $f \in k(a_1, \ldots, a_n)[y]$ s.t. $f(b_{r+1}) = 0$. Getting rid of the denominators of the polynomial we can without loss of generality assume that the coefficients of f are in the form of $P(a_1, \ldots, a_n)$, i.e. we have nonzero $g \in k[x_1, \ldots, x_n, y]$ s.t. $g(a_1, \ldots, a_n, b_{r+1}) = 0$ via evaluating f on b_{r+1} on the coefficients given by g. Since $b_1, \ldots, b_r, b_{r+1}$ are algebraically independent over k. Without loss of generality we can assume that x_n appears with nonzero coefficient in g. Now write

$$g = \sum_{i=0}^{p} g_i(x_1, \ldots, x_{n-1}, y) x_n^i$$

If there exists j s.t. $g_j(a_1, \ldots, a_{n-1}, b_{r+1}) \neq 0$, then a_n is algebraic over $k(a_1, \ldots, a_{n-1}, b_{r+1})$. This gives the algebraic extension

$$k(a_1, \ldots, a_{n-1}, b_{r+1}) \hookrightarrow k(a_1, \ldots, a_n, b_{r+1}) \hookrightarrow K$$

Otherwise there exists $g_j \neq 0$ s.t. $g_j(a_1, \ldots, a_{n-1}, b_{r+1}) = 0$. Repeat the process with g replaced with g_j. This process must terminate as $g \neq 0$. □

Corollary 9.10. Every two transcendental basis of K over k have the same number of elements (or are in bijection, for the infinite case).

Proposition 9.11. If $K = k(a_1, \ldots, a_n)$, then there exists a subset $A \subseteq \{a_1, \ldots, a_n\}$ that is a transcendental basis over k. In particular, $\mathrm{trdeg}(K/k) \leq n$.

Proof. Let $A \subseteq \{a_1, \ldots, a_n\}$ be the maximal subset which is algebraically independent (which exists by Proposition 9.5). But by Proposition 9.4 this implies that if $a_i \notin A$, then a_i is algebraic over $k(A)$. Therefore, $k(A) \hookrightarrow K = k(a_1, \ldots, a_n)$ is algebraic, i.e. A is a transcendental basis. □

Proposition 9.12. If we have $k \hookrightarrow K \hookrightarrow L$ field extensions, then $\mathrm{trdeg}(L/k) = \mathrm{trdeg}(K/k) + \mathrm{trdeg}(L/K)$.

Proof. First deal with the cases where RHS is infinite:

– If $\mathrm{trdeg}(K/k)$ is infinite, then a transcendental basis for K/k is part of a transcendental basis of L/k as L can be viewed as a vector space over K.

– If $\mathrm{trdeg}(L/K)$ is infinite, then in a transcendental basis for L/K are in particular algebraically independent over k, which implies that $\mathrm{trdeg}(L/k)$ is infinite.

Now we may assume that we have a finite transcendental basis $a_1, \dots, a_m$ for K/k and $b_1, \dots, b_n$ for L/K. Claim that $\{a_1, \dots, a_m, b_1, \dots, b_n\}$ gives a transcendental basis of L/k. Verify the followings:

1) The sub-extensions are algebraic since a_is and b_is are transcendental bases for the corresponding extensions (by Theorem 9.6)

$$k(a_1, \dots, a_m, b_1, \dots, b_n) \hookrightarrow K(b_1, \dots, b_n) \hookrightarrow L$$

By Proposition 4.15 we have the extension $L/k(a_1, \dots, a_m, b_1, \dots, b_n)$ being algebraic.

2) The set $\{a_1, \dots, a_m, b_1, \dots, b_n\}$ is algebraically independent over k. Proceed to show by induction on i for $0 \leq i \leq n$ that $\{a_1, \dots, a_m, b_1, \dots, b_i\}$ are algebraically independent over k:

For $i = 0$ the result is clear by hypothesis. For the inductive step it suffices to show that b_{i+1} is not algebraically dependent on $\{a_1, \dots, a_m, b_1, \dots, b_i\}$, then by Proposition 9.4 we have the set $\{a_1, \dots, a_m, b_1, \dots, b_i, b_{i+1}\}$ algebraically independent over k. This is clear as b_js give a transcendental basis over K, and are therefore algebraically independent over k. Taking $i = n$ gives the algebraic independence over k.

□

Verify that we indeed have the desired properties of transcendental degree as mentioned in the beginning of the section:

1) $\mathrm{trdeg}(K/k) = 0$ if and only if the extension $k \hookrightarrow K$ is algebraic. This comes as a corollary of Proposition 9.6.

2) $K = k(a_1, \dots, a_n)$ if and only if $\mathrm{trdeg}(K/k) \leq n$, with equality if and only if a_is are algebraically independent. This results from Theorem 9.9.

3) The proposition above (Proposition 9.12) gives the additivity of transcendental degree.

Remark 9.13. The results above implies that $k(x_1, \dots, x_m) \simeq k(x_1, \dots, x_n)$ as k-algebras (where x_is are formal variables) if and only if $m = n$. Notice that for $m \neq n$ they can still be isomorphic as fields: take $k = \mathbb{Q}(x_1, x_2, \dots)$ (with infinitely many variables) and let $m = 0$ and $n = 1$, with the isomorphism $x_i \mapsto x_{i+1}$. But this is clearly not k-linear.

Definition 9.14 (Purely Transcendental)**.** A finitely generated field extension K/k is **purely transcendental** if $K \simeq k(x_1, \dots, x_n)$ as k-algebras for some n.

This is somewhat related to ring theory: we state without proof the following results:

Definition 9.15 (Dimension (Ring))**.** Given a commutative ring R, its **dimension** is defined as

$$\dim R := \sup_n \{n \mid \exists\, p_0 \subsetneqq \cdots \subsetneqq p_n,\ p_i \subseteq R \text{ prime ideals}\}$$

Theorem 9.16. Given a field k and a domain R, if R is a finitely generated k-algebra, then $\dim R = \operatorname{trdeg}(\operatorname{Frac}(R)/k)$.

10 The Fundamental Theorem of Galois Theory

We now return to the discussion of Galois Theory. We have introduced the Galois Group of a field extension $k \hookrightarrow K$:

$$G(K/k) := \{\sigma \in \operatorname{Aut}(K) \mid \sigma(u) = u, \forall u \in k\}$$

The following section seeks to establish the relation between the structure of the Galois Group and the corresponding field extension.

Proposition 10.1. If $K = k(\alpha)$, then $|G(K/k)| \leq [K : k]$ with equality if and only if K/k is normal, and α is separable over k.

Proof. Every k-algebra homomorphism $\sigma : K \hookrightarrow \bar{K}$ is uniquely determined by $\sigma(\alpha)$; and if $f \in k[x]$ is the minimal polynomial of α, by Corollary 8.5 σ permutes the roots of f in $\bar{K}$. Then we have the chain of inequalities:

$$|G(K/k)| \leq \left|\{\sigma : K \to \bar{K} \mid \sigma \text{ is a morphism of } k\text{-algebra}\}\right| \leq \#\text{ distinct roots of } f \leq \deg f = [K : k]$$

and we have equalities when f is separable, and K is the splitting field of f. □

Theorem 10.2 (Fundamental Theorem of Galois Theory)**.** Let K/k be a finite Galois extension. Then we have two maps:

$$\{k \hookrightarrow L \hookrightarrow K\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \{\text{subgroups of } G = G(K/k)\}$$

where $\Phi(L) = G(K/L)$, and for $H \leq G$, $\Psi(H) = K^H := \{u \in K \mid \sigma(u) = u, \forall \sigma \in H\}$. They further satisfy the following two properties:

1) Φ and Ψ are order-reversing, inverse bijections.
2) $H \leq G$ is a normal subgroup if and only if $k \hookrightarrow K^H$ is a normal extension. In this case, the group homomorphism

$$G(K/k) \to G(K^H/k), \qquad \sigma \mapsto \sigma|_{K^H}$$

induces an isomorphism $G/H \simeq G(K^H/k)$.

Remark 10.3. We first consider some simple examples of such correspondence:

1) The correspondence is *order-reversing*: If $H_1 \leq H_2 \leq G$, then $K^{H_2} \subseteq K^{H_1}$ (as H_2 fixes fewer elements); and for $k \hookrightarrow L_1 \hookrightarrow L_2 \hookrightarrow K$, $G(K/L_2) \leq G(K/L_1)$.
2) For simplicity in the followings we will write K^H for $\Psi(H)$. Notice for $H \leq G$, $H \leq G(K/K^H)$, as K^H by definition is the set of elements fixed by H; and in the other direction for extensions $k \hookrightarrow L \hookrightarrow K$, $G(K/L)$ fixes L. We need to prove the equality.

Before proving the main theorem we need some more tools to describe $[K : K^H]$ for $H \leq G(K/k)$:

Proposition 10.4. Given a field K and a group G, any mutually distinct group homomorphisms $\chi_1, \dots, \chi_n : G \to K^\times$ are linearly independent as elements of $\mathrm{Func}(G; K)$ as a K-vector space.

Proof. Prove by contradiction. Suppose that we have a relation $\sum_{i=1}^n a_i\chi_i = 0$, with not all a_is being zero. Without loss of generality, assume n is minimal, i.e. all a_is are nonzero. Separate the cases:

- $n = 1$. Then $a_1\chi_1 = 0$; but since $\chi_1 \in K^\times$ which cannot be zero, $a_1 = 0$. Contradiction.
- $n > 1$. By definition we have
$$\sum_{i=1}^n a_i\chi_i(g) = 0 \quad \forall g \in G \tag{$*$}$$
Since χ_is are distinct, there exists $h \in G$ s.t. $\chi_1(h) \neq \chi_n(h)$. Fix h, and choose $g \in G$ arbitrarily. Since χ_is are group homomorphisms, we have by linear independence
$$\sum_{i=1}^n a_i\chi_i(hg) = 0 = \sum_{i=1}^n a_i\chi_i(h)\chi_i(g) \qquad \forall g \in G$$
Multiplying $\chi_1(h)$ on the right of Eq. ($*$), and subtract the RHS of the equality above, we have
$$\sum_{i=0}^n a_i \underbrace{(\chi_i(h) - \chi_1(h))}_{\text{zero iff } i=1} \chi_i(g) = 0 \qquad \forall g \in G$$
which contradicts the minimality of n.

□

Corollary 10.5. If $\sigma_1, \dots, \sigma_n \in \mathrm{Aut}(K)$ are distinct group homomorphisms, and K is a field, then $\sigma_1, \dots, \sigma_n$ are linearly independent in $\mathrm{Func}(K; K)$ viewed as a K-vector space.

Proof. $\sigma_1|_{K^\times}, \cdots, \sigma_n|_{K^\times}$ are distinct group automorphisms on $K^\times$. Apply the above proposition. □

Proposition 10.6. Let K be a field, and $A \subseteq \mathrm{Aut}(K)$ a subset. For $L = \{u \in K \mid \sigma(u) = u, \forall u \in A\}$, $[K : L] \geq |A|$.

Proof. May assume that $[K : L] = n$ is finite, and $u_1, \dots, u_n$ is a basis of K over L (as a L-vector space).

Argue by contradiction: suppose that we have $\sigma_1, \dots, \sigma_{n+1} \in A$ distinct. Consider the system of linear equations over L:
$$\sum_{i=1}^{n+1} \sigma_i(u_j)x_i = 0, \qquad 1 \leq j \leq n$$
This is a system with n equations and $(n + 1)$ variables, which must exist a nontrivial solution $(a_1, \dots, a_{n+1})$. Since u_is give a basis of K over L, this is equivalent to having
$$\sum_{i=1}^{n+1} a_i\sigma_i(u_j) = 0 \ (\forall j) \implies \sum_{i=1}^{n+1} a_i\sigma_i = 0$$
contradicting Corollary 10.5. □

Proposition 10.7. If $A \subseteq \mathrm{Aut}(K)$ is a finite group, with the same notation as above we have equality $[K : L] = |A|$.

Proof. It is already proven that $[K : L] \geq |A|$. Now suppose that $[K : L] > |A|$ for $A = \{\sigma_1, \ldots, \sigma_d\}$. Then there exists elements $u_1, \ldots, u_{d+1} \in K$ that are linearly independent over L.

Apply the similar strategy as before. Consider the linear system of equations over K:

$$\sum_{i=1}^{d+1} \sigma_j(u_i)x_i = 0, \qquad 1 \leq j \leq d$$

As there are d equations with $d+1$ variables, there exists a nontrivial solution $(a_1, \ldots, a_{d+1})$ s.t.

$$\sum_{i=1}^{d+1} a_i\sigma(u_i) = 0 \qquad \forall \sigma \in A$$

In particular we can ignore all nonzero a_is and get L-linearly independent elements $u_1, \ldots, u_m$ in K s.t.

$$\sum_{i=1}^{m} a_i\sigma(u_i) = 0 \qquad a_i \neq 0\ (\forall i),\ m \text{ minimal} \tag{$*$}$$

Then either

- $m = 1$. $a_1\sigma(u_1) = 0$. Take in particular $\sigma = \mathrm{Id}$, this gives $a_1u_1 = 0 \implies u_1 = 0$ but this contradicts with $\{u_1\}$ being linearly independent.
- $m > 1$. Multiply Eq. ($*$) by a_1^{-1} on the left, we can assume that $a_1 = 1$. Further take $\sigma = \mathrm{Id}$ in Eq. ($*$), we have $\sum_{i=1}^m a_iu_i = 0$. Suppose that all a_is are nonzero. Since u_is are linearly independent over L, after reordering we may assume that $a_m \notin L$ (otherwise $\{u_m\}$ is not linearly independent). Then there exists $\tau \in A$ s.t. $\tau(a_m) \neq a_m$. Applying τ to Eq. ($*$) gives (recalling that τ is a group homomorphism)

  $$\sum_{i=1}^{m} \tau(a_i)\underbrace{\tau\sigma}_{\text{runs through } A}(u_i) = 0\ (\forall \sigma \in A) \implies \sum_{i=1}^{m} \tau(a_i)\sigma(u_i) = 0\ (\forall \sigma \in A)$$

  Subtracting Eq. ($*$) gives (recalling that without loss of generality we may assume $a_1 = 1$, and τ is an automorphism on K)

  $$\sum_{i=1}^{m} \underbrace{(\tau(a_i) - a_i)}_{\text{zero iff } i=1} \sigma(u_i) = 0 \qquad \forall \sigma \in A$$

  which contradicts the minimality of m.

□

We now use the above results to prove the main theorem:

Proof of Theorem 10.2. □

11 Norm and Trace Maps

12 Solvability by Radicals