In this course a ring will always be commutative with a 1, i.e., a set \( R \) and two operations \(+\), \( \times\) such that:

- \((R, +)\) is an abelian group —
  - A1 \((x + y) + z = x + (y + z)\) \(\text{Associativity}\)
  - A2 \(x + y = y + x\) \(\text{Commutativity}\)
  - A3 \(x + 0 = 0 + x = x\) \(\text{Additive Identity}\)
  - A4 \(x + (-x) = (-x) + x = 0\) \(\text{Additive Inverse}\)

- \((R, \times)\) is a commutative semigroup —
  - M1 \((xy)z = x(yz)\) \(\text{Associativity}\)
  - M2 \(xy = yx\) \(\text{Commutativity}\)
  - M3 \(x1 = 1x = x\) \(\text{Multiplicative Identity}\)

- Multiplication by \(x \in R\) is an endomorphism of \((R, +)\) —
  - D1 \(x(y + z) = xy + xz, (y + z)x = yx + zx\) \(\text{Distributivity}\)

A field is a non-trivial ring with multiplicative inverses:

- M4 \(xx^{-1} = x^{-1}x = 1\) \(\text{(for } x \neq 0\text{)}\) \(\text{Multiplicative Inverse}\)

An Integral Domain (ID) is a non-trivial ring with either of the two equivalent conditions:

- ID \(xy = 0 \Rightarrow x = 0\) or \(y = 0\) \(\text{No zero divisors}\)
- ID' \(xy = xz\) and \(x \neq 0 \Rightarrow y = z\) \(\text{Cancellation law}\)

Note that any field is an ID and any subring of a ID (or field) is an ID.

Examples

1. \(\{0\}\) is the trivial ring, the only ring with \(1 = 0\). By convention we do not regard it as being an ID or a field.
2. \(\mathbb{Z}\) is an ID. \(\mathbb{Q}\), \(\mathbb{R}\), and \(\mathbb{C}\) are fields.
3. \(\mathbb{Z}/n\mathbb{Z}\) is a ring for any \(n > 0\). It is not an ID unless \(n\) is prime, however if \(n = p\) is prime then it is a field which we denote by \(\mathbb{F}_p\).
4. If \(R\) is a ring then so is the polynomial ring \(R[X] = \{\sum_{i=0}^n a_i X^i : a_i \in R, \ n \in \mathbb{N}\}\). If \(R\) is an ID then so is \(R[X]\), but \(R[X]\) is never a field.
5. If \(R\) is an ID then the field of fractions \(\text{Frac } R\) is the set of quotients \{(\text{a/b : a, b \in R, b \neq 0})\} modulo the equivalence relation \(a/b = c/d\) iff \(ad = bc\). \(\text{Frac } R\) is a field and is the smallest field containing \(R\) as a subring (i.e., any field with \(R\) as a subring contains a subfield \(F \supseteq R\) isomorphic to \(\text{Frac } R\)). For example, \(\text{Frac } \mathbb{Z} = \mathbb{Q}\).
6. If \(F\) is a field, \(F(X) = \text{Frac } F[X]\) is the field of rational functions over \(F\) and consists of all quotients of polynomials \(f(X)/g(X)\) with \(g(X) \neq 0\).

A ring homomorphism is a map \(\phi: R \rightarrow S\) such that \(\phi(x + y) = \phi(x) + \phi(y), \phi(xy) = \phi(x)\phi(y)\), and \(\phi(1) = 1\).
An ideal of $R$ is an additive subgroup $I$ of $R$ such that $ra \in I$ for all $a \in I$, $r \in R$. An ideal $I$ is proper if $I \neq R$.

If $I$ is an ideal of $R$ then the quotient ring $R/I$ is the group of additive cosets $a + I$ with multiplication given by $(a + I)(b + I) = ab + I$.

A subring of $R$ is an additive subgroup $S$ of $R$ such that $1 \in S$ and $ab \in S$ for all $a, b \in S$. A subfield is a subring that is a field.

The 1st Isomorphism Theorem states that if $\phi: R \to S$ is a ring homomorphism then $\text{Ker} \phi = \{a : \phi(a) = 0\}$ is an ideal of $R$, $\text{Im} \phi = \{\phi(a) : a \in R\}$ is a subring of $S$, and $R/\text{Ker} \phi \cong \text{Im} \phi$.

Examples

1. If $S$ is a subset of $R$ then $(S) = \{\sum_{i=1}^{n} r_ia_i : r_i \in R, a_i \in S\}$ is the smallest ideal of $R$ containing $S$. An ideal of the form $(a) = \{ra : r \in R\}$ is called a principal ideal.

2. If $R$ is a field then the only ideals of $R$ are $(0)$ and $R$. In particular a ring homomorphism from a field to a non-trivial ring is always injective.

3. If $\phi: R \to S$ is a homomorphism and $\alpha \in S$ then the evaluation map $ev_{\phi,\alpha}: R[X] \to S$ given by $ev_{\phi,\alpha}(\sum a_iX^i) = \sum \phi(a_i)\alpha^i$ is a ring homomorphism. If $\phi$ is the identity, we write $ev_{\phi,\alpha}(f)$ as $f(\alpha)$.

A proper ideal $I$ is prime if $ab \in I$ implies either $a \in I$ or $b \in I$. Equivalently, $R/I$ is an ID.

A proper ideal $I$ is maximal if $I \subseteq J$ implies $J = I$ or $J = R$. Equivalently, $R/I$ is a field.

The element $a$ divides the element $b$, $a \mid b$, if $\exists c : b = ca$. Equivalently, $b \in (a)$, or $(b) \subseteq (a)$.

An element $a$ is a unit if it is invertible, $\exists b : ab = 1$. Equivalently, $a \mid 1$, or $(a) = R$.

A non-zero non-unit element $a$ of an ID is prime if $a \mid bc$ implies $a \mid b$ or $a \mid c$. Equivalently, $(a)$ is a non-zero prime ideal.

A non-zero non-unit element $a$ of an ID is irreducible if $a = bc$ implies either $b$ or $c$ is a unit. Equivalently, $(a)$ is maximal among the set of proper principal ideals.

Note: $I$ maximal $\implies$ $I$ prime, $a$ prime $\implies$ $a$ irreducible.

A Principal Ideal Domain (PID) is an ID in which every ideal is principal. Examples include $\mathbb{Z}$ and $F[X]$ for any field $F$. For a PID we have the following equivalences:

$a$ is irreducible $\iff$ $a$ is prime $\iff$ $(a)$ is a non-zero prime ideal $\iff$ $(a)$ is maximal.

If $R$ is a ring, then the image of the homomorphism $f: \mathbb{Z} \to R; m \mapsto m.1$ is called the prime subring of $R$. The prime subring is the smallest subring of $R$ and is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for some $n$. In the first case we say $R$ has characteristic zero, char $R = 0$. In the second case we say $R$ has characteristic $n$, char $R = n$. If $R$ is an ID then char $R$ is either 0 or prime.

If $F$ is a field, the prime subfield is the smallest subfield of $F$. It is isomorphic to the field of fractions of the prime subring, and so is isomorphic to either $\mathbb{Q}$ (if char $F = 0$), or $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (if char $F = p$).
A vector space $V$ over the field $F$ or an $F$-vector space $V$ is an additive abelian group $(V, +)$ together with a scalar multiplication map $F \times V \to V; (\lambda, v) \mapsto \lambda v$ satisfying the following properties:

V1 $\forall \lambda, \mu \in F, v \in V : (\lambda + \mu)v = \lambda v + \mu v$
V2 $\forall \lambda \in F, u, v \in V : \lambda(u + v) = \lambda u + \lambda v$
V3 $\forall \lambda, \mu \in F, v \in V : (\lambda \mu)v = \lambda(\mu v)$
V4 $\forall v \in V : 1v = v$

The first two axioms state that scalar multiplication is an additive homomorphism in each variable if the other variable is fixed. The last two axioms state that scalar multiplication gives a group action of the group $(F \setminus \{0\}, \times)$ on the set $V$. Note that V1 with $\lambda = 0$ implies that $0v = 0$ for all $v$.

If we replace the field $F$ by an arbitrary ring $R$ then the axioms V1–V4 define an $R$-module.

A set $S \subseteq V$ is called linearly independent if there are no finite non-trivial linear combinations that give 0. In other words if $\sum_{i=1}^{n} \lambda_i s_i = 0$ and the $s_i$ are distinct elements of $S$ then $\lambda_i = 0$ for each $i$.

A set $S \subseteq V$ is called spanning if every element $v \in V$ can be written as a finite linear combinations of elements of $S$, $v = \sum_{i=1}^{n} \lambda_i s_i$.

A set $S \subseteq V$ is called a basis if it is a linearly independent spanning set. Note that every element $v \in V$ can be written as a linear combination of elements of a basis in a unique way. (Spanning implies existence, linear independence implies uniqueness.)

**Theorem 1** If $I \subseteq S \subseteq V$, $I$ is linearly independent, and $S$ spans $V$, then there exists a basis $B$ of $V$ with $I \subseteq B \subseteq S$.

By taking $I = \emptyset$ or $S = V$ we conclude that any independent set can be enlarged to form a basis and any spanning set can be reduced to form a basis. Taking $I = \emptyset$ and $S = V$ we see that any vector space has a basis. The proof uses Zorn’s Lemma in general.

**Theorem 2** If $B$ and $B'$ are two bases of $V$ then $|B| = |B'|$ (finite or infinite).

If $|B|$ is infinite then the proof requires Zorn’s Lemma. The cardinality $|B|$ is called the dimension of $V$ and is denoted $\dim V$ or $\dim_F V$. 
A field extension $K/F$ is an (injective) ring homomorphism between two fields $i: F \to K$, so identifies $F$ with the subfield $i(F)$ of $K$. When the map $i$ is clear, we often abuse notation by regarding $F$ as a subset of $K$. E.g., $\mathbb{C}/\mathbb{R}$ is a field extension and we commonly write $\mathbb{R} \subset \mathbb{C}$.

If $K/F$ is an extension then we can regard $K = (K,+)$ as a vector space over $F$ since the map $F \times K \to K$ which sends $(x,y)$ to $xy = i(x)y$ satisfies the axioms V1–V4. The dimension of this vector space is called the degree of $K$ over $F$, $[K:F] = \dim_F K$. An extension $K/F$ is called finite if $[K:F] < \infty$.

**Examples** $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{Q}(X)/\mathbb{Q}$ are field extensions. $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$ ($\{1, \pi, \pi^2, \ldots\}$ is linearly independent over $\mathbb{Q}$), $[\mathbb{Q}(X) : \mathbb{Q}] = \infty$ ($\{1, X, X^2, \ldots\}$ is linearly independent over $\mathbb{Q}$).

**Theorem (The Tower Law)** If $L/K$ and $K/F$ are field extensions then $L/F$ is a field extension and $[L:F] = [L:K][K:F]$ (finite or infinite).

**Proof.** We can compose the inclusions $F \to K$ and $K \to L$ to get an inclusion $F \to L$. Hence $L/F$ is an extension. Let $\{a_i : i \in I\}$ be a basis for $K/F$ and $\{b_j : j \in J\}$ be a basis for $L/K$.

The result will follow if we can show that $\{a_ib_j : i \in I, j \in J\}$ is a basis for $L/F$.

**Independence:** If $\sum_{ij} \lambda_{ij}a_ib_j = 0$ with $\lambda_{ij} \in F$ then $\mu_j = \sum_i \lambda_{ij}a_i \in K$ and $\sum_j \mu_jb_j = 0$. By independence of the $b_j$ we have $\mu_j = 0$, and then by independence of the $a_i$ we have $\lambda_{ij} = 0$.

**Spanning:** If $\alpha \in L$ we can write $\alpha = \sum_j \mu_jb_j$ for some $\mu_j \in K$. But then we can write $\mu_j = \sum_i \lambda_{ij}a_i$ with $\lambda_{ij} \in F$, so $\alpha = \sum_{ij} \lambda_{ij}a_ib_j$. \qed

**Corollary** $L/F$ is finite iff both $L/K$ and $K/F$ are finite.

Recall that if $R$ is a subring of $R'$ and $S \subseteq R'$ then we denote by $R[S]$ the smallest subring of $R'$ containing $R$ and $S$. More explicitly, $R[S] = \{f(s_1, \ldots, s_n) : f \in R[X_1, \ldots, X_n], s_i \in S, n \in \mathbb{N}\}$.

If $K/F$ is an extension and $S \subseteq K$, denote by $F(S)$ the smallest subfield of $K$ containing both $F$ and $S$. Note that $F(S) = \text{Frac}(F[S]) = \{f(s_1, \ldots, s_n)/g(s_1, \ldots, s_n) : f,g \in F[X_1, \ldots, X_n], g(s_1, \ldots, s_n) \neq 0\}$. We write $F(a)$ for $F(\{a\})$ etc..

The extension $K/F$ is called simple if $K = F(a)$ for some $a \in K$. In this case $a$ is called a primitive element of $K/F$.

**Examples** $\mathbb{C}/\mathbb{R}$ is simple since $\mathbb{C} = \mathbb{R}(i)$. $\mathbb{R}/\mathbb{Q}$ is not simple since $\mathbb{Q}(a)$ is a countable set for all $a \in \mathbb{R}$ but $\mathbb{R}$ is uncountable.

**Warning:** Whenever you write $R[a,b,\ldots]$ or $F(a,b,\ldots)$ it is important that you work inside some fixed, specified ring $R'$ or field $K$.

**Exercises**

1. Show that $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{C}$ has degree 2 over $\mathbb{Q}$ and $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.

2. Show that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ and $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$.

3. Deduce that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ and give a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.

4. Show that if $F$ is a finite field then $|F| = p^n$ for some prime $p$ and integer $n > 0$. 
Definition Let \( K/F \) be a field extension. We say \( \alpha \in K \) is algebraic over \( F \) if there exists a non-zero polynomial \( f \in F[X] \) with \( f(\alpha) = 0 \). Otherwise we call \( \alpha \) transcendental over \( F \). We say \( K \) is algebraic over \( F \) if every \( \alpha \in K \) is algebraic over \( F \). Otherwise we call \( K \) transcendental over \( F \).

Examples The real number \( \sqrt{2} \) is algebraic over \( \mathbb{Q} \) (take \( f = X^2 - 2 \)) and \( \pi \) is transcendental over \( \mathbb{Q} \). However \( \pi \) is algebraic over \( \mathbb{R} \) (take \( f = X - \pi \in \mathbb{R}[X] \)). Since \( \mathbb{R} \) contains at least one element that is transcendental over \( \mathbb{Q} \), \( \mathbb{R}/\mathbb{Q} \) must be transcendental. The extension \( \mathbb{C}/\mathbb{R} \) is algebraic since for any \( z \in \mathbb{C} \) we can take \( f = X^2 - (z + \bar{z})X + z\bar{z} \in \mathbb{R}[X] \).

Theorem 1 Let \( K/F \) be a field extension and let \( \alpha \in K \). The following are equivalent:

A1 the element \( \alpha \) is algebraic over \( F \),
A2 \( \ker \text{ev}_\alpha = (m_{\alpha,F}) \) for some unique monic irreducible polynomial \( m_{\alpha,F} \in F[X] \),
A3 for \( f \in F[X] \), \( f(\alpha) = 0 \) iff \( m_{\alpha,F} \mid f \),
A4 \( F[\alpha] = F(\alpha) \) and both are isomorphic to \( F[X]/(m_{\alpha,F}) \),
A5 \( [F(\alpha):F] = \deg m_{\alpha,F} = n < \infty \) and the set \( \{1, \alpha, \ldots, \alpha^{n-1}\} \) is a basis for \( F(\alpha)/F \).

Conversely, if these conditions do not hold then:

T1 the element \( \alpha \) is transcendental over \( F \),
T2 \( \ker \text{ev}_\alpha = (0) \),
T3 for \( f \in F[X] \), \( f(\alpha) = 0 \) iff \( f = 0 \),
T4 \( F[\alpha] \neq F(\alpha), F[\alpha] \cong F[X], \) and \( F(\alpha) \cong F(X) = \text{Frac} F[X] \).
T5 \( [F(\alpha):F] = \infty \).

The polynomial \( m_{\alpha,F} \) is called the minimal polynomial of \( \alpha \) over \( F \).

Examples \( \mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i], m_{i,\mathbb{R}} = X^2 + 1, [\mathbb{C} : \mathbb{R}] = \deg m_{i,\mathbb{R}} = 2, \) and \( \{1, i\} \) is a basis for \( \mathbb{C}/\mathbb{R} \). Note that \( m_{i,\mathbb{C}} = X - i \neq m_{i,\mathbb{R}}, \) so it is important to specify the ground field \( F \).

Theorem 2 If \( K/F \) is finite then it is algebraic. [Converse not true in general.]

Proof. If \( \alpha \in K \) and \( [K : F] = n \) then \( \{1, \alpha, \alpha^2, \ldots, \alpha^n\} \) is linearly independent in the \( F \)-vector space \( K \). Hence there exists \( \lambda \in F \) such that \( \sum_{i=0}^n \lambda_i \alpha^i = 0 \) and not all \( \lambda_i \) are zero. Hence \( f(\alpha) = 0 \) where \( f = \sum_{i=0}^n \lambda_i X^i \in F[X], f \neq 0 \). Thus \( \alpha \) is algebraic over \( F \).

Theorem 3 If \( A \) is the set of all elements of \( K \) algebraic over \( F \) then \( A \) is a subfield of \( K \) containing \( F \).

Proof. The elements of \( F \) are algebraic over \( F \), so \( F \subseteq A \subseteq K \). If \( \alpha, \beta \in A \) then \( \alpha \) is algebraic over \( F \) and \( \beta \) is algebraic over \( F(\alpha) \) (since \( \beta \) is algebraic over \( F \)). Hence \( [F(\alpha, \beta):F] = [F(\alpha, \beta):F(\alpha)][F(\alpha):F] = (\deg m_{\beta,F(\alpha)})(\deg m_{\alpha,F}) < \infty \). Therefore \( F(\alpha, \beta) \) is algebraic over \( F \) and so \( \alpha \pm \beta, \alpha/\beta, \alpha \beta \in F(\alpha, \beta) \) are algebraic over \( F \). Hence \( \alpha \pm \beta, \alpha/\beta, \alpha \beta \in A \) and \( A \) is a subfield of \( K \).
Theorem 4 If \( L/K/F \) then \( L/F \) is algebraic iff both \( L/K \) and \( K/F \) are.

Proof. \( \Rightarrow \) is clear. Now assume both \( L/K \) and \( K/F \) are algebraic and \( \alpha \in L \). Then \( f(\alpha) = 0 \) where \( f = \sum_{i=0}^{n} b_i X^i \in K[X], f \neq 0 \). Define \( F_i = F(b_0, \ldots, b_{i-1}) \). Then \( \alpha \) is algebraic over \( F_{n+1} \) (since \( f \in F_{n+1}[X] \) and \( f(\alpha) = 0 \)), \( b_i \) is algebraic over \( F_i \) (since \( b_i \in K \) is algebraic over \( F \)), and \( F_{i+1} = F_i(b_i) \). Hence \( [F_{n+1}(\alpha) : F] = [F_{n+1}(\alpha) : F_{n+1}] [F_{n+1} : F_n] \cdots [F_1 : F_0] < \infty \). Therefore \( \alpha \in F_{n+1}(\alpha) \) is algebraic over \( F = F_0 \).

Constructive proof of Theorems 3 and 4.

Suppose \( \alpha, \beta \in K \) are both algebraic over \( F \). Theorem 3 states that combinations such as \( \alpha + \beta \) and \( \alpha \beta \) are also algebraic over \( F \), but the proof does not indicate how to find an \( f \) such that \( f(\alpha + \beta) = 0 \) or \( f(\alpha \beta) = 0 \). It is possible however to make Theorem 3 constructive.

Theorem (Symmetric Function Theorem) If \( f \in R[X_1, \ldots, X_n] \) is symmetric under interchange of any pair \( X_i, X_j \), then \( f \in R[\sigma_1, \ldots, \sigma_n] \) where \( \sigma_i \) is the \( i \)th elementary symmetric function of the \( X_i \).

Suppose there exists \( M/K \) such that \( m_\alpha = m_{\alpha,F} \) and \( m_\beta = m_{\beta,F} \) split in \( M \), i.e., factor completely into linear factors \( m_\alpha = (X - \alpha_1) \cdots (X - \alpha_m), m_\beta = (X - \beta_1) \cdots (X - \beta_m) \), \( \alpha = \alpha_1, \beta = \beta_1, \alpha_1, \beta_1 \in M \). (We shall prove the existence of such an \( M \) later, the \( \alpha_i \) are called the conjugates of \( \alpha \)). Now consider the polynomial

\[
f(X) = \prod_{i=1}^{n} \prod_{j=1}^{m} (X - \alpha_i \beta_j) \in F[\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m, X] \subseteq M[X].
\]

We can consider \( f \) as a polynomial in indeterminates \( \alpha_i \) and coefficients in \( R = F[\beta_1, \ldots, \beta_m, X] \). By the Symmetric Function Theorem, \( f \in R[\sigma_1, \ldots, \sigma_m] \), where \( \sigma_i \) are the elementary symmetric functions in the \( \alpha_i \). But then \( \sigma_i \) are just \( \pm \) the coefficients of \( m_\alpha \), so lie in \( F \). Thus \( f \in F[\beta_1, \ldots, \beta_m, X] \). A similar argument using symmetry in the \( \beta_j \) shows that \( f \in F[X] \). But \( f \) is monic (so non-zero) and \( f(\alpha \beta) = f(\alpha_1 \beta_1) = 0 \). Hence \( \alpha \beta \) is algebraic over \( F \). Note that \( f \) might not be irreducible so we can only conclude that \( m_{\alpha \beta,F} \) is a factor of \( f \).

A similar argument can be used for \( \alpha \pm \beta \). For \( 1/\alpha \) the proof is easier since we can take the polynomial \( f(X) = X^n m_\alpha(1/X) \). Hence Theorem 3 can be made constructive.

For Theorem 4 a similar trick can be used. Let \( \alpha \) be algebraic over \( K \) with minimal polynomial, \( m_{\alpha,K} = \sum_{i=0}^{m} \beta_i X^i \), where each \( \beta_i \) is algebraic over \( F \). Suppose we can find a \( M/L \) such that each minimal polynomial \( m_{\beta_i,F} \) splits, \( m_{\beta_i,F} = \prod_{j=1}^{n} (X - \beta_{i,j}) \), \( \beta_i = \beta_{i,1}, \beta_{i,j} \in M \). Now consider

\[
f(X) = \prod_{j_1=1}^{n_1} \cdots \prod_{j_m=1}^{n_m} \sum_{i=0}^{m} \beta_{i,j_1} \cdots \beta_{i,j_m} X^i \in F[\beta_{1,1}, \ldots, \beta_{1,n_1}, \beta_{2,1}, \ldots, \beta_{m,n_m}, X].
\]

This polynomial is symmetric in each collection \( \{ \beta_{i,1}, \ldots, \beta_{i,n_i} \} \), so by applying the Symmetric Function Theorem \( m \) times we get \( f \in F[X] \). But \( m_{\alpha,K} \mid f \), so \( f(\alpha) = 0 \).
Definition If \( P \) and \( Q \) are two distinct points of \( \mathbb{R}^2 \), write \( L(P,Q) \) for the (infinite) line through \( P \) and \( Q \) and \( C(P,Q) \) for the circle with center \( P \) going through the point \( Q \).

Definition The point \( P \in \mathbb{R}^2 \) is constructible by ruler and compass from the set of points \( \{P_1, \ldots, P_n\} \) if there is a sequence of points \( P_{n+1}, P_{n+2}, \ldots, P_m = P \), where each \( P_i, i > n \) is constructed from previous points using one of the following constructions:

1. \( P_i \) is the point of intersection of two distinct lines of the form \( L(P_j, P_k), j,k < i \),
2. \( P_i \) is any point of intersection of two distinct circles of the form \( C(P_j, P_k), j,k < i \),
3. \( P_i \) is any point of intersection of a line \( L(P_j, P_k) \) and a circle \( C(P_r, P_s), j,k,r,s < i \).

We say a line (resp. circle) is constructible if it is of the form \( L(P,Q) \) (resp. \( C(P,Q) \)) for some pair of constructible points \( P \) and \( Q \). If \( n = 1 \) then the only constructible point is \( P_1 \), hence we may assume \( n \geq 2 \). Define a Cartesian coordinate system so that \( P_1 = (0,0) \) and \( P_2 = (1,0) \).

Lemma 1 The set of constructible points is of the form \( \mathcal{C} = \{(x,y) : x, y \in F\} \) where \( F \) is some subfield of \( \mathbb{R} \). Moreover, if \( a \in F \) and \( a > 0 \) then \( \sqrt{a} \in F \).

Proof Let \( F = \{x : (x,0) \text{ is constructible}\} \).

Step 1. If \( P, Q \in \mathcal{C} \) then the line perpendicular to \( L(P,Q) \) through \( P \) is constructible. \[ L(P,Q) \cap C(P,Q) = \{Q, R\}, S \in C(R,Q) \cap C(Q,R), L(P,S) \text{ is perpendicular to } L(P,Q).\] Call this line \( L^\perp(P,Q) \).

Step 2. If \( (x,0), (y,0) \in \mathcal{C} \) then \( (x,y) \in \mathcal{C} \). \[ (0, y) \in C((0,0),(y,0)) \cap L^\perp((0,0),(1,0)), L^\perp((0,y),(0,0)) \cap L^\perp((x,0),(0,0)) = \{(x,y)\}.\]

Step 3. If \( P, Q, R \in \mathcal{C} \) then the projection of \( R \) onto \( L(P,Q) \) is constructible. \[ C(P,R) \cap C(Q,R) = \{R, S\}, L(R,S) \cap L(P,Q) = \{T\}.\]

Step 4. If \( (x, y) \in \mathcal{C} \) then \( (x,0), (y,0) \in \mathcal{C} \). \[ \text{Project } (x, y) \text{ onto } L((0,0),(1,0)) \text{ and } L^\perp((0,0),(1,0)) \text{ (the axes) to get } (x,0) \text{ and } (0,y). \]

Steps 2 and 4 imply that \( \mathcal{C} = \{(x,y) : x, y \in F\} \).

Step 5. If \( x, y \in F \) then \( x \pm y \in F \). \[ C((x,0),(x,y)) \cap L((0,0),(1,0)) = \{(x+y,0),(x-y,0)\}.\]

Step 6. If \( x, y \in F \) and \( x \neq 0 \) then \( y/x, xy \in F \). \[ L((0,0),(x,y)) \cap L^\perp((1,0),(0,0)) = \{(1,y/x)\}. \text{ Also } y/(1/x) = xy.\]

We have now shown that \( F \) is a field.

Step 7. If \( x \in F, x > 0 \), then \( \sqrt{x} \in F \). \[ C((x-1)/2,0),(x,0) \cap L^\perp((0,0),(1,0)) = \{(0,\pm\sqrt{x})\}. \]
Lemma 2 If $K/F$ is an extension with $[K:F] = 2$ and $\text{char } F \neq 2$ then $K = F(\sqrt{\alpha})$ for some $\alpha \in F$.

**Proof.** Pick any $\beta \in K$, $\beta \notin F$. Then $[F(\beta):F] > 1$, so $F(\beta) = K$, and $\deg m_{\beta,F} = 2$. Hence $\beta$ is the solution to a quadratic equation $m_{\beta,F} = aX^2 + bX + c = 0$ with coefficients in $F$. Hence $\beta$ can be written in terms of a square root of an element $\alpha = b^2 - 4ac \in F$. Conversely $\sqrt{\alpha}$ can be written in terms of $\beta$, so $F(\sqrt{\alpha}) = F(\beta) = K$. \hfill \square

**Theorem 1** A point $(x,y)$ is constructible from $\{P_1, \ldots, P_n\}$, $P_0 = (0,0)$, $P_1 = (1,0)$, $P_i = (x_i,y_i)$, $i \geq 2$, iff there exists a sequence of fields $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m \subseteq \mathbb{R}$ with $F_0 = \mathbb{Q}(x_2,y_2,\ldots,x_n,y_n)$, $[F_{i+1}:F_i] = 2$, and $x,y \in F_m$.

**Proof.** Let $F_m$ be as described above and let $F$ be defined as in Lemma 1. Then $x_i,y_i \in F$, $i = 2, \ldots, n$, so $F \supseteq F_0$. Also, $[F_{i+1}:F_i] = 2$, so by Lemma 2, $F_{i+1} = F_i(\sqrt{\alpha})$ for some $\alpha \in F_i$ and $\alpha > 0$ (since $F_{i+1} \subseteq \mathbb{R}$). Hence by induction $F \supseteq F_i$. Thus $x,y \in F_m \subseteq F$ and $(x,y)$ is constructible. Conversely suppose $(x,y)$ is constructible, it is enough to show that if the coordinates of $P_1, \ldots, P_{i-1}$ lie in $K$ and $P_i = (x,y)$ is the intersection of lines and/or circles formed from $P_j$, $j < i$, then $[K(x,y):K] \leq 2$. If $P,Q \in K^2$, then $L(P,Q)$ is given by an equation of the form $ax + by + c = 0$ where $a,b,c \in K$. Similarly $C(P,Q)$ is a circle of the form $x^2 + y^2 + ax + by + c = 0$, $a,b,c \in K$. It is easy to check that the $x$ and $y$ coordinates of an intersection of such lines and circles can be obtained by solving a linear or quadratic equation. Hence $[K(x,y):K] \leq 2$. \hfill \square

As a consequence of Theorem 1 and the Tower Law, if $(x,y)$ is constructible then $[F_0(x,y):F_0]$ is a power of 2, or equivalently, if $\alpha \in F$ then $[F_0(\alpha):F_0]$ is a power of 2.

**Examples**

1. The cube cannot be doubled.
   The aim is to construct a length $\sqrt[3]{2}$ times longer than a given length $P_0P_1$. This would imply $\sqrt[3]{2} \in F$ which is impossible since $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ is not a power of 2.

2. The circle cannot be squared.
   The aim is to construct a length $\sqrt[4]{\pi}$ times longer than a given length $P_0P_1$. This would imply $\pi \in F$ which is impossible since $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$ is not a power of 2.

3. In general, the trisection of an angle is not constructible.
   An angle is given by three points $P_0, P_1, P_2$ where $P_0 = (0,0)$, $P_1 = (1,0)$, and $P_2 = (x,y)$ where $y/x = \tan \theta$. An easy exercise shows that $a = 2\cos \theta \in F$, and conversely the point $P_3$ can be chosen as $(\cos \theta, \sin \theta)$, so that $[F_0:Q(a)] \leq 2$. If there are constructible points $Q_1, Q_2, Q_3$ that make an angle $\theta/3$ then an easy exercise shows that $\alpha = 2\cos(\theta/3) \in F$. [If the $Q_i$ are constructible, then so are $Q_2 - Q_1$ and $Q_3 - Q_1$. By intersecting with $C((0,0), (1,0))$ we see that the sines and cosines of the angles $\theta_2, \theta_3$ that $L(Q_1, Q_2)$ and $L(Q_1, Q_3)$ make with the $x$-axis lie in $F$. Using trigonometric identities gives $\alpha = 2\cos(\theta_3 - \theta_2) \in F$.] Hence $[Q(a)(\alpha) : Q(a)]$ is a power of 2. By the triple angle formula for cosines, $\alpha$ is a root of $X^3 - 3X - a = 0$. There are many choices for $a$ that make this polynomial irreducible over $Q(a)$, for example $a = 1 (\theta = 60^\circ)$. But then $[Q(a)(\alpha) : Q(a)] = 3$, a contradiction.
We start with a rather technical, but very useful, lemma.

Lemma (Artin’s Extension Theorem) Let \( \phi : F_1 \to F_2 \) be an isomorphism of fields. Let \( K_1/F_1 \) and \( K_2/F_2 \) be two extensions and let \( \alpha \in K_1 \). Then there is an extension of \( \phi \) to \( \tilde{\phi} : F_1(\alpha) \to K_2 \) with \( \tilde{\phi}|_{F_1} = \phi \) and \( \tilde{\phi}(\alpha) = \beta \in K_2 \) iff \( \beta \) is a zero of \( \phi(m_{\alpha,F_1}) \in F_2[X] \). Moreover, for each such \( \beta \) \( \tilde{\phi} \) is unique.

[If \( f \in F_1[X] \) then \( \phi(f) \in F_2[X] \) is obtained by applying \( \phi \) to the coefficients of \( f \). In terms of our earlier notation, \( \phi(f) = \text{ev}_{\phi,X}(f) \).]

Proof. Write \( m_{\alpha,F_1} = \sum b_i X^i \). If \( \tilde{\phi} \) exists and \( \beta = \tilde{\phi}(\alpha) \) then \( \phi(m_{\alpha,F_1})(\beta) = \sum \phi(b_i)\beta^i = \sum \phi(b_i)\tilde{\phi}(\alpha)^i = \phi(\sum b_i \alpha^i) = \tilde{\phi}(0) = 0 \). Also, \( \tilde{\phi} \) is unique since every element of \( F_1(\alpha) \) can be written in the form \( f(\alpha), f \in F_1[X] \), and \( \tilde{\phi}(f(\alpha)) = \phi(f)(\beta) \) is uniquely determined. Conversely, assume \( \beta \) is a zero of \( \phi(m_{\alpha,F_1}) \), then \( m_{\beta,F_2} = \phi(m_{\alpha,F_1}) \) since the latter is monic and irreducible. Now both \( \text{ev}_{1,\alpha} : F_1[X] \to F_1(\alpha) \) and \( \text{ev}_{\phi,\beta} : F_1[X] \to F_2(\beta) \) are surjective with kernel \( (m_{\alpha,F_1}) \) and we can define \( \tilde{\phi} \) as the composition of the two isomorphisms

\[ F_1(\alpha) \cong F_1[X]/(m_{\alpha,F_1}) \cong F_2(\beta). \]

Under this isomorphism \( \alpha \mapsto X + (m_{\alpha,F_1}) \mapsto \beta \) and \( c \mapsto c + (m_{\alpha,F_1}) \mapsto \phi(c) \) for \( c \in F_1 \).

We shall often use this lemma with \( F_1 = F_2 \) and \( \phi = 1 \). Note that the image of \( \tilde{\phi} \) is \( F_2(\beta) \), so \( \tilde{\phi} \) gives an isomorphism \( F_1(\alpha) \to F_2(\beta) \).

Examples

1. The fields \( \mathbb{Q}(\sqrt{2}) \) and \( \mathbb{Q}(i\sqrt{2}) \) are isomorphic, but distinct, subfields of \( \mathbb{C} \).
2. There is an automorphism of \( \mathbb{Q}(\sqrt{2}) \) sending \( \sqrt{2} \) to \( -\sqrt{2} \) and fixing \( \mathbb{Q} \).

Definition A polynomial \( f(X) \in F[X] \) splits in \( K/F \) if it factors as a product of linear factors in \( K[X] \).

Examples

1. The polynomial \( X^2 - 2 \) splits in \( \mathbb{Q}(\sqrt{2}) \).
2. The polynomial \( X^3 - 2 \) has a zero, but does not split in \( \mathbb{Q}(\sqrt{2}) \) since \( \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R} \), but only one of the three roots of \( X^3 - 2 = 0 \) is real.

Definition A splitting field extension (sfe) of \( f \in F[X] \) is an extension \( K/F \) such that

(a) \( f \) splits in \( K \), and
(b) if \( F \subseteq L \subseteq K \) and \( f \) splits in \( L \) then \( L = K \).

More generally, a splitting field extension of \( \mathcal{F} \subseteq F[X] \) is an extension \( K/F \) such that

(a) \( f \) splits in \( K \) for all (non-zero) \( f \in \mathcal{F} \), and
(b) if \( F \subseteq L \subseteq K \) and \( f \) splits in \( L \) for all \( f \in \mathcal{F} \) then \( L = K \).
Theorem 1 If \( f \in F[X] \) then there exists an extension \( K/F \) in which \( f \) splits. Moreover, if \( \deg f = n \) then such a \( K \) exists with \( [K:F] \leq n! \).

**Proof.** We proceed by induction on \( n \). Let \( g \) be an irreducible factor of \( f \) in \( F[X] \). Let \( F' = F[X]/(g) \). Then \( (g) \) is a maximal ideal, \( F' \) is a field, and \( F'/F \) is a field extension. Let \( \alpha = X + (g) \in F' \). Then \( g(\alpha) = 0 \) in \( F' \). Thus \( f(\alpha) = 0 \) and we can write \( f(X) = (X - \alpha)h(X) \) in \( F'[X] \). Applying induction, there exists an extension \( K/F' \) in which \( h(X) \) splits and \( [K:F'] \leq (n-1)! \). But then \( f(X) \) splits in \( K \) and \( [K:F] = [K:F'][F':F] \leq n! \). \( \square \)

We can extend this theorem to any finite set \( \mathcal{F} \) of polynomials by considering the polynomial \( f(X) = \prod_{g \in \mathcal{F} \setminus \{0\}} g(X) \in F[X] \). For infinite \( \mathcal{F} \) one needs Zorn’s lemma to find \( K \).

Theorem 2 If every \( f \in \mathcal{F} \) splits in \( K \) then there exists a unique subfield \( L \subseteq K \) such that \( L/F \) is a sfe for \( \mathcal{F} \).

**Proof.** Let \( A = \{ \alpha \in K : \alpha \) is a zero of some \( f \in \mathcal{F} \} \). If \( L \subseteq K \) is a sfe of \( \mathcal{F} \) then \( A \subseteq L \) and \( F \subseteq L \). Hence \( L \supseteq F(A) \). Conversely, every \( f \in \mathcal{F} \) splits in \( F(A) \). Hence \( L = F(A) \) is the unique subfield of \( K \) that is a sfe for \( \mathcal{F} \). \( \square \)

Theorem 3 Any two sfe’s for \( f \in F[X] \) are isomorphic.

**Proof.** We shall prove a slightly stronger result: If \( \phi : F \rightarrow F' \) is an isomorphism, \( K \) is a sfe of \( f \in F[X] \), and \( \phi(f) \) splits in \( K'/F' \), then there is an extension \( \tilde{\phi} : K \rightarrow K' \) of \( \phi \).

Let \( g \) be a monic irreducible factor of \( f \) and let \( \alpha \) be a zero of \( g \) in \( K \) and \( \beta \) a zero of \( \phi(g) \) in \( K' \). By Artin’s extension Theorem, \( \phi \) extends to an isomorphism \( \phi' : F(\alpha) \rightarrow F'(\beta) \). Write \( f(X) = (X - \alpha)h(X) \) in \( F(\alpha)[X] \). Now \( K/F(\alpha) \) is a sfe for \( h \) and \( \phi'(h) \) splits in \( K' \) (since \( \phi'(h) | \phi(f) \)). Hence by induction on \( \deg f \), \( \phi' \) extends to a map \( \tilde{\phi} : K \rightarrow K' \).

Now assume \( K' \) is also a sfe and \( F = F' \). Then \( f \) splits in \( \text{Im} \tilde{\phi} \subseteq K' \). Hence \( \text{Im} \tilde{\phi} = K' \) and \( \tilde{\phi} \) is an isomorphism. \( \square \)

Putting Theorems 1–3 together, we see that a sfe for \( f \in F[X] \) exists, is unique up to isomorphism, has degree at most \( n! \) over \( F \), and can be written as \( K = F(\alpha_1, \ldots, \alpha_n) \) where \( \alpha_1, \ldots, \alpha_n \) are the zeros of \( f \) in \( K \).

**Examples**

1. The sfe of \( X^3 - 2 \) over \( \mathbb{Q} \) is \( \mathbb{Q}(\sqrt[3]{2}, \zeta_3 \sqrt[3]{2}, \zeta_3^2 \sqrt[3]{2}) = \mathbb{Q}(\zeta_3, \sqrt[3]{2}) \), where \( \zeta_3 = e^{2\pi i/3} \). This extension is of degree 6 = 3! over \( \mathbb{Q} \). [Prove this!]

2. The sfe of \( X^3 - 2 \) over \( \mathbb{R} \) is \( \mathbb{C} \), which is of degree 2 < 3! over \( \mathbb{R} \).

**Exercise:** Find the sfe \( K \) of \( X^4 - 2 \) over \( \mathbb{Q} \). What is \( [K: \mathbb{Q}] \)?
A partial ordering on a set $\mathcal{X}$ is a relation $\leq$ satisfying the properties

O1 $\forall x : x \leq x$,
O2 $\forall x, y : if \ x \leq y \ and \ y \leq x \ then \ x = y$,
O3 $\forall x, y, z : if \ x \leq y \ and \ y \leq z \ then \ x \leq z$.

A total ordering is a partial ordering which also satisfies

O4 $\forall x, y : either \ x \leq y \ or \ y \leq x$.

Examples Any collection of sets with $\subseteq$ as the ordering forms a partially ordered set that is not in general totally ordered. The usual $\leq$ on $\mathbb{R}$ is a total ordering.

If $(\mathcal{X}, \leq)$ is a partially ordered set, a chain in $\mathcal{X}$ is a non-empty subset $T \subseteq \mathcal{X}$ that is totally ordered by $\leq$.

If $T \subseteq \mathcal{X}$, and $x \in \mathcal{X}$, we say $x$ is an upper bound for $T$ if $y \leq x$ for all $y \in T$. [Note that we do not require $x$ to be an element of $T$, for example, $2 \in \mathbb{R} = \mathcal{X}$ is an upper bound for $T = [0,1]$.

A maximal element of $\mathcal{X}$ is an element $x$ such that for any $y \in \mathcal{X}$, $x \leq y$ implies $x = y$. [Note: This does not imply that $y \leq x$ for all $y$ since $\leq$ is only a partial order. In particular there may be many maximal elements.]

Theorem (Zorn’s Lemma) If $(\mathcal{X}, \leq)$ is a non-empty partially ordered set for which every chain has an upper bound then $\mathcal{X}$ has a maximal element.

This result follows from (and is equivalent to) the Axiom of choice, which states that if $X_i$ are non-empty sets then $\prod_{i \in I} X_i$ is non-empty. [I will not give the proof here as it is rather long.]

Note: If we had defined things so that $\emptyset$ were a chain, we would not need the condition that $\mathcal{X} \neq \emptyset$ in Zorn’s Lemma since the existence of an upper bound for $\emptyset$ is just the condition that an element of $\mathcal{X}$ exists. However, in practice it is easier to check $\mathcal{X} \neq \emptyset$ and then check separately that each non-empty totally ordered subset has an upper bound.

Examples

Theorem If $I$ is a proper ideal of a ring $R$ (with 1) then there exists a maximal ideal $M$ such that $I \subseteq M$.

Proof. If an ideal $J$ contains 1 then $J = R$, so an ideal is proper iff it does not contain 1. Let $\mathcal{X} = \{J : J$ is a proper ideal of $R$ with $I \subseteq J\}$. The partial order on $\mathcal{X}$ will be $\subseteq$. Since $I \in \mathcal{X}$, $\mathcal{X} \neq \emptyset$. Now let $T$ be a chain in $\mathcal{X}$, i.e., a set of ideals $\{J_\alpha\}$ such that for every $J_\alpha, J_\beta \in T$ either $J_\alpha \subseteq J_\beta$ or $J_\beta \subseteq J_\alpha$. We shall show that $K = \bigcup_{J_\alpha \in T} J_\alpha$ is an upper bound for $T$.

Firstly $T \neq \emptyset$, so some ideal $J_\alpha$ lies in $T$ and $I \subseteq J_\alpha \subseteq K$. In particular $K \neq \emptyset$. If $x, y \in K$ then $x \in J_\alpha$, $y \in J_\beta$, say. Since $T$ is totally ordered, we can assume without loss of generality that $J_\alpha \subseteq J_\beta$. Thus $x, y \in J_\beta$, and $x - y \in J_\beta \subseteq K$. If $x \in K$, $r \in R$, then $x \in J_\alpha$, say, so $xr, rx \in J_\alpha \subseteq K$. Hence $K$ is an ideal with $I \subseteq K$. However $1 \notin J_\alpha$ for each $J_\alpha \in T$, so $1 \notin K$.

Hence $K$ is proper. Therefore $K \in \mathcal{X}$ and is clearly an upper bound for $T$. 

Spring 2003
The conditions of Zorn’s Lemma apply, so $\mathcal{X}$ has a maximal element $M$, say. Now $M$ is a proper ideal containing $I$ and is maximal, since if $M \subset J \subset R$ then $J \in \mathcal{X}$ and $M$ would not be maximal in $\mathcal{X}$. □

We now give an example from linear algebra. Let $V$ be a vector space (possibly infinite dimensional).

A set $S \subseteq V$ is called linearly independent if there are no non-trivial finite linear combinations that give 0. In other words if $\sum_{i=1}^{n} \lambda_i s_i = 0$ and the $s_i$ are distinct elements of $S$ then $\lambda_i = 0$ for each $i$.

A set $S \subseteq V$ is called spanning if every element $v \in V$ can be written as a finite linear combinations of elements of $S$, $v = \sum_{i=1}^{n} \lambda_i s_i$.

A set $S \subseteq V$ is called a basis if it is a linearly independent spanning set. Note that every element $v \in V$ can be written as a linear combination of elements of a basis in a unique way. [Spanning implies existence, linear independence implies uniqueness.]

**Theorem** Every vector space has a basis.

**Proof.** Let $\mathcal{X}$ be the set of all linearly independent sets in $V$ partially ordered by $\subseteq$. Since $\emptyset$ is linearly independent, $\mathcal{X} \neq \emptyset$. Let $T$ be a chain in $\mathcal{X}$ and let $S = \cup_{S_\alpha \in T} S_\alpha$. We shall show that $S$ is linearly independent.

Suppose $\sum_{i=1}^{n} \lambda_i s_i = 0$ and $s_i \in S_i \in T$ (the $s_i$ are distinct but the $S_i$ need not be distinct). Then by total ordering of the $S_i$, there must be one $S_{i_0}$ that contains all the others (use induction on $n$). But then $\sum_{i=1}^{n} \lambda_i s_i = 0$ is a linear relation in $S_{i_0}$ which is linearly independent. Thus $\lambda_i = 0$ for all $i$. Hence $S$ is linearly independent, so $S \in \mathcal{X}$ and is clearly an upper bound for $T$.

Now apply Zorn’s Lemma to give a maximal linearly independent set $M$. We shall show that $M$ spans $V$ and so is a basis. Clearly any element of $M$ is a linear combination of elements of $M$, so pick any $v \notin M$ and consider $M \cup \{v\}$. By maximality of $M$ this cannot be linearly independent. Hence there is a linear combination $\lambda v + \sum_{i=1}^{n} \lambda_i s_i = 0$, $s_i \in M$, with not all the $\lambda$’s zero. If $\lambda = 0$ this gives a linear relation in $M$, contradicting linear independence of $M$. Hence $\lambda \neq 0$ and $v = \sum_{i=1}^{n} (-\lambda_i/\lambda) s_i$ is a linear combination of elements of $M$. □

**Note:** If $I \subseteq S$ and $I$ is a linearly independent set and $S$ is a spanning set then the above proof can be modified to give a basis $M$ with $I \subseteq M \subseteq S$. Just let $\mathcal{X}$ be the linearly independent subsets of $S$ containing $I$ and in the last paragraph pick $v \in S \setminus M$. [If $S \subseteq M$ then $M$ clearly spans $V$.]
The aim is to use Zorn’s Lemma to prove, given \( F \), the existence and uniqueness of the splitting field extension of any \( \mathcal{F} \subseteq F[X] \). We need to generalize Theorems 1 and 3 above (Theorem 2 already applies to any \( \mathcal{F} \)).

**Theorem 1’** For any field \( F \), there exists an extension \( K/F \) in which every \( f \in F[X] \) splits.

The idea of the proof is to use Zorn’s Lemma to construct a “maximal” algebraic extension. Unfortunately the collection of algebraic extensions do not form a set, so we have to be a bit more careful. In particular, we need to fix the underlying set of elements of the extensions, so that the collection of extensions forms a well defined set.

**Proof.** Let \( \mathcal{L} \) be the set of ordered pairs \((f, n)\) where \( f \in F[X] \) is a monic irreducible polynomial and \( n \in \mathbb{N} \). This will be our underlying set. An \( \mathcal{L} \)-extension (not standard notation) will be a field \((K, +, \times)\) where

1. \( K \subseteq \mathcal{L} \),
2. the map \( i: F \to K \) given by \( i(a) = (X - a, 1) \) is a ring homomorphism (so \( K/F \) is an extension and \( F \) can be identified with the set \( \{(X - a, 1) : a \in F \} \subseteq K \) ),
3. if \( \alpha = (f, n) \in K \) then \( f(\alpha) = 0 \) (where the coefficients \( c_i \) of \( f \) are identified with \( i(c_i) \in K \)).

It is clear that any algebraic extension is isomorphic to one of this form. Indeed, if \( M/F \) is an algebraic extension we can just rename the roots \( \alpha_1, \ldots, \alpha_r \) of any irreducible polynomial \( f = m_{\alpha_1,F} \) as \((f, 1), \ldots, (f, r)\). Since each \( f \) has only finitely many roots we never run out of elements of \( \mathcal{L} \). [Technically this requires the axiom of choice since there are an infinite number of choices as to how to do the renaming: for each \( f \) we must order the roots.]

Let \( \mathcal{X} \) be the set of all \( \mathcal{L} \)-extensions. It is clear that \( \mathcal{X} \) is a set. Indeed, it is a subset of \( \mathcal{P}(\mathcal{L}) \times \mathcal{P}(\mathcal{L} \times \mathcal{L} \times \mathcal{L}) \times \mathcal{P}(\mathcal{L} \times \mathcal{L} \times \mathcal{L}) \) where \( \mathcal{P}(A) \) denotes the set of all subsets of \( A \). [We regard + and \( \times \) as subsets of \( \mathcal{L} \times \mathcal{L} \times \mathcal{L} \), since they can be determined by the set of all triples \((a, b, a + b)\) or \((a, b, ab)\).]

Define a partial order on \( \mathcal{L} \)-extensions by setting \((K, +, \times) \leq (K', +', \times')\) iff \( K \) is a subfield of \( K' \), i.e., \( K \subseteq K' \) and + and \( \times \) are the restrictions of +’ and \times’ to \( K \). It is clear that \( \leq \) is a partial order.

The field \( \{(X - a, 1) : a \in F\} \) with \((X - a, 1) + (X - b, 1) = (X - (a + b), 1) \) and \((X - a, 1)(X - b, 1) = (X - ab, 1) \) is an \( \mathcal{L} \)-extension, so \( \mathcal{X} \neq \emptyset \). Let \( \mathcal{T} \) be a chain in \( \mathcal{X} \). We claim that \( \bigcup_{K \in \mathcal{T}} K \in \mathcal{X} \). If \( \alpha, \beta \in \bigcup_{K \in \mathcal{T}} K \) then \( \alpha \in K_1 \), \( \beta \in K_2 \) for some \( K_1, K_2 \in \mathcal{T} \). Since \( \mathcal{T} \) is totally ordered, we can assume \( K_1 \leq K_2 \), so \( \alpha, \beta \in K_2 \). Define \( \alpha + \beta \) and \( \alpha \beta \) by their values in \( K_2 \). Then by the definition of \( \leq \), these values agree with their values in any \( K \in \mathcal{T} \) with \( K_2 \leq K \). The field axioms follow immediately, since to check an axiom, we just take any \( K \in \mathcal{T} \) big enough to contain all the relevant elements and use the corresponding axioms in \( K \). The fact that \( a \mapsto (X - a, 1) \) is a ring homomorphism and \( f(\alpha) = 0 \) when \( \alpha = (f, n) \) follow from the corresponding properties in each \( K \in \mathcal{T} \). It is now clear that \( \bigcup_{K \in \mathcal{T}} K \) is an upper bound for \( \mathcal{T} \). Zorn’s Lemma now provides us with the existence of a maximal \( \mathcal{L} \)-extension, \((M, +, \times)\) say.
We now prove that every $f \in \mathbb{F}[X]$ splits in $M$. If not, then there exists a sfe for $f$ over $M$, say $M'/M$ with $M' \neq M$. But $M'/M$ and $M/F$ are algebraic, so $M'/F$ is algebraic. By renaming the elements of $M'$ we can assume $M \subseteq M'$. By renaming the elements $\alpha \in M' \setminus M$ as $(m_{\alpha,F},i)$ as above, we can assume that $M'$ is an $L$-extension containing $M$. Note that we never run out of choices for $i$ since every $m_{\alpha,F}$ has only finitely many roots. Clearly $M \subseteq M'$ and $M \neq M'$ contradicting the choice of $M$. Hence every polynomial in $\mathbb{F}[X]$ splits in $M$.

\textbf{Theorem 3'} If $K/F$ and $M/F$ are extensions with $K/F$ an sfe for $\mathbb{F} \subseteq \mathbb{F}[X]$ and assume $\mathbb{F}$ splits in $M$. There exists an homomorphism $\phi: K \to M$ that fixes $F$. In particular, if $M/F$ is also an sfe for $\mathbb{F}$ then $\phi$ is an isomorphism.

\textit{Proof.} Let $\mathcal{X}$ be the set of homomorphisms $\phi: L_\phi \to M$ where $L_\phi$ is some subfield of $K$ containing $F$ and $\phi$ fixes $F$. The inclusion $F \to M$ lies in $\mathcal{X}$, so $\mathcal{X} \neq \emptyset$. Define a partial ordering on $\mathcal{X}$ by $\phi \leq \psi$ if $L_\phi \subseteq L_\psi$ and $\phi = \psi$ on $L_\phi$. This is clearly a partial order. Let $T$ be a chain in $\mathcal{X}$. Define $\tilde{L}$ to be $\bigcup_{\phi \in T} L_\phi$. Since the $L_\phi$ are totally ordered by inclusion, $\tilde{L}$ is a subfield of $K$ containing $F$. [If $\alpha, \beta \in \tilde{L}$ then $\alpha \in L_\phi, \beta \in L_\psi$ for some $\phi, \psi \in T$. Since $T$ is totally ordered, we may assume $\phi \leq \psi$, so $\alpha, \beta \in L_\psi$. Then $\alpha \pm \beta, \alpha \beta, \alpha/\beta \in L_\psi \subseteq \tilde{L}$.] Define $\tilde{\phi}(a)$ to be $\phi(a)$ for any $\phi \in T$ for which $a \in L_\phi$. Since $T$ is totally ordered, if $a \in L_\phi, L_\psi$ we can assume $\phi \leq \psi$ and so $\phi(a) = \psi(a)$. Hence $\tilde{\phi}$ is well defined. It is obvious that $\tilde{\phi}$ is a ring homomorphism from $\tilde{L}$ to $M$, so $\tilde{\phi} \in \mathcal{X}$ and it is clearly an upper bound for $T$. Now using Zorn’s Lemma we have a maximal $\phi \in T$.

If $L_\phi \neq K$ then some $f \in \mathbb{F}$ does not split in $L_\phi$. Hence there exists a root $\alpha$ of $f$ with $\alpha \in K$ and $\alpha \notin L_\phi$. Let $m_\alpha$ be the minimal polynomial of $\alpha$ over $L_\phi$. Note that $m_\alpha | f$. Let $L' = \text{Im}(\phi)$ be the image of $L_\phi$ in $M$. Then $L'$ is a subfield of $M$, isomorphic (via $\phi$) to $L_\phi$. The image $\phi(m_\alpha)$ is therefore irreducible in $L'[X]$. Since $m_\alpha | f, \phi(m_\alpha) | \phi(f) = f$, so $\phi(m_\alpha)$ must split in $M$ (since $f$ does). Therefore there exists a $\beta \in M$ which is a root of $\phi(m_\alpha)$. The minimal polynomial of $\beta$ over $L'$ is clearly $\phi(m_\alpha)$, so by Artin’s extension Theorem, there exists a $\hat{\phi}: L_\phi(\alpha) \to M$ which agrees with $\phi$ on $L_\phi$. Hence $\hat{\phi} \in \mathcal{X}$ and $\phi < \hat{\phi}$ contradicting the choice of $\phi$. Therefore $L_\phi = K$.

Finally, since $K$ is isomorphic to the image $\text{Im} \phi$, $\mathbb{F}$ splits in $\text{Im} \phi/F$ and $\text{Im} \phi \subseteq M$. If $M/F$ is a sfe, $\text{Im} \phi = M$ and $\phi$ gives an isomorphism from $K$ to $M$ fixing $F$.

\textbf{Lemma 1} If $K/F$ is an extension, then $K$ is a sfe for $\mathbb{F} = \mathbb{F}[X]$ iff (a) $K/F$ is algebraic and (b) every non-constant $f \in \mathbb{F}[X]$ has a root in $K$.

\textit{Proof.} Assuming (a) and (b) and using induction on $\deg f$ we see that every $f \in \mathbb{F}[X]$ splits in $K$. But every element of $K$ is a root of some $f \in \mathbb{F}[X]$ so $K$ must be a sfe for $\mathbb{F}[X]$. Conversely, if $K$ is the sfe for $\mathbb{F}[X]$ then $K/F$ is algebraic and if $f \in \mathbb{F}[X]$ is irreducible, $M = \mathbb{F}[X]/(f)$ is an algebraic extension of $K$. But then $M/F$ is algebraic, so every $\alpha \in M$ is a root of some $g \in \mathbb{F}[X]$. But then $\alpha \in K$, so $M = K$ and $f$ is linear. In particular every non-constant polynomial in $\mathbb{F}[X]$ factors into linear factors, so has a root in $K$.

The extension $K$ of Lemma 1 is called the \textit{algebraic closure} of $\mathbb{F}$ and is denoted $\overline{\mathbb{F}}$. The above theorems show that the algebraic closure exists and is unique up to isomorphism.
Definition  An extension $K/F$ is normal iff $K/F$ is algebraic and if any irreducible $f \in F[X]$ has a root in $K$ then it splits in $K$.

**Theorem 1** Assume $K/F$ is an extension. The following are equivalent:

(a) $K/F$ is normal,

(b) $K/F$ is a sfe for some $\mathcal{F} \subseteq F[X]$,

(c) the extension $K/F$ is algebraic and if $M$ is any field and $\phi, \psi : K \rightarrow M$ are any two homomorphisms with $\phi|_F = \psi|_F$ then $\text{Im } \phi = \text{Im } \psi$.

**Proof.** (a)$\Rightarrow$(b): Assume $K/F$ is normal and let $\mathcal{F} = \{m_{\alpha,F} : \alpha \in K\}$. Then every $f \in \mathcal{F}$ splits in $K$, so $\mathcal{F}$ splits in $K$. Conversely, if $L \subseteq K$ and $\mathcal{F}$ splits in $L$ then $L$ contains all the roots of each $m_{\alpha,F}$. Hence $L$ contains each $\alpha \in K$. Therefore $L = K$ and $K$ is a sfe for $\mathcal{F}$.

(b)$\Rightarrow$(c): Both $\text{Im } \phi$ and $\text{Im } \psi$ are subfields of $M$ and are sfe's for $\phi(\mathcal{F}) = \psi(\mathcal{F})$. Hence $\text{Im } \phi = \text{Im } \psi$.

(c)$\Rightarrow$(a): Assume $K/F$ is not normal. Then there exists an irreducible $f \in F[X]$ such that $f$ has a root $\alpha \in K$ but does not split over $K$. Let $M$ be a sfe over $K$ for the set $\mathcal{F} = \{m_{\gamma,F} : \gamma \in K\}$. Now without loss of generality $f = m_{\alpha,F}$, so $f$ splits in $M$. Let $\beta$ be another root of $f$ that does not lie in $K$. By Artin, there exists an isomorphism $\phi : F(\alpha) \rightarrow F(\beta)$ fixing $F$. Now $M/F(\alpha)$ and $M/F(\beta)$ are sfe's for $\mathcal{F}$ and $\phi(\mathcal{F}) = \mathcal{F}$ respectively. Hence $\phi$ extends to an isomorphism $\tilde{\phi} : M \rightarrow M$ with $\tilde{\phi}(\alpha) = \beta$. Now $\tilde{\phi}|_K$ and the inclusion $i : K \rightarrow M$ are two maps $K \rightarrow M$ with distinct images since $\beta \in \text{Im } \tilde{\phi}|_K$ but $\beta \notin \text{Im } i$. This contradicts (c), so $K/F$ is normal. □

**Definition** Let $K/F$ be algebraic. Then $M$ is a normal closure of $K/F$ iff $M$ is an extension of $K$ such that (a) $M/F$ is normal, and (b) if $K \subseteq L \subseteq M$ and $L/F$ is normal then $L = M$.

**Lemma 2** Let $K/F$ be algebraic and $K = F(A)$ for some subset $A \subseteq K$. Then $M/K$ is a normal closure of $K/F$ iff $M$ is a sfe for $\mathcal{F} = \{m_{\alpha,A} : \alpha \in A\}$ over $K$ (or over $F$).

**Proof.** Let $M/K$ be a normal closure of $K/F$. Then every $m_{\alpha,F} \in \mathcal{F}$ has a root $\alpha \in K \subseteq M$. Hence every $m_{\alpha,F}$ splits in $M$. Let $L \subseteq M$ be a sfe for $\mathcal{F}$ over $F$. Then $L$ contains all the roots of every $m_{\alpha,F} \in \mathcal{F}$. In particular $A \subseteq L$, so $F(A) = K \subseteq L$. This implies $L$ is a sfe for $\mathcal{F}$ over $K$ as well. Also $L/F$ is a sfe, so is normal. Thus by the definition of normal closure $L = M$. Now let $M/K$ be a sfe for $\mathcal{F}$. Let $L \subseteq M$ be a sfe for $\mathcal{F}$ over $F$. Then $A \subseteq L$, $F(A) = K \subseteq L$ and $L$ is a sfe for $\mathcal{F}$ over $K$. Hence $L = M$ and $M/F$ is normal. Now let $K \subseteq L' \subseteq M$ with $L'/F$ normal. Since every $m_{\alpha,F} \in \mathcal{F}$ has a root $\alpha \in K \subseteq L'$, it must split in $L'$. Therefore $\mathcal{F}$ splits in $L'$ and $L' = M$ by definition of sfe. □

**Corollary 3** Normal closures exist and are unique up to isomorphism. Also, if $[K:F] < \infty$ and $M/K$ is a normal closure of $K/F$ then $[M:F] < \infty$.

**Proof.** Existence and uniqueness up to isomorphism follow since $M/K$ is a sfe for some $\mathcal{F}$. If $[K:F] < \infty$ then $K = F(A)$ for some finite set $A$ (e.g., let $A$ be a basis for the vector space $K$ over $F$). Hence $M/F$ is a sfe for a finite set of polynomials and so $[M:F] < \infty$. □

**Examples** The normal closure of $Q(\sqrt{2})/Q$ is equal to the sfe of $m_{\sqrt{2},Q} = X^4 - 2$ over $Q(\sqrt{2})$ (or $Q$), which is $Q(\sqrt{2}, i\sqrt{2}, i^2 \sqrt{2}, i^3 \sqrt{2}) = Q(\sqrt{2}, i)$. 

Spring 2003
Lemma 1 Let $K_1/F_1$ and $K_2/F_2$ be extensions with $[K_1:F_1] < \infty$. Let $\phi: F_1 \to F_2$ be an isomorphism. Then

$$|\{\tilde{\phi}: K_1 \to K_2 : \tilde{\phi}|_{F_1} = \phi\}| \leq [K_1:F_1].$$

Moreover if $K_1 = F_1(A)$ then equality holds iff $\phi(m_{\alpha,F_1})$ splits in $K_2[X]$ into distinct linear factors for all $\alpha \in A$.

Proof. Proof is by induction on $[K_1:F_1]$. When $[K_1:F_1] = 1$ the result is clear. Now assume $[K_1:F_1] > 1$ and pick some $\alpha \in A$, $\alpha \not\in F_1$. Now let $\beta_1, \ldots, \beta_r \in K_2$ be the (distinct) roots of $\phi(m_{\alpha,F_1})$ in $K_2$. By Artin's extension theorem, for each $i = 1, \ldots, r$ there exists an isomorphism $\phi_i: F_1(\alpha) \to F_2(\beta_i)$ given by $\phi_i(\alpha) = \beta_i$. By induction each $\phi_i$ can be extended to at most $[K_1:F_1(\alpha)]$ maps $\tilde{\phi}: K_1 \to K_2$. Conversely any map $\tilde{\phi}: K_1 \to K_2$ gives by restriction to $F_1(\alpha)$ one of the maps $\phi_i$. Therefore the number of $\tilde{\phi}$s is at most $[K_1:F_1(\alpha)]r$. But $r \leq \deg m_{\alpha,F_1} = [F_1(\alpha):F_1]$, so there are at most $[K_1:F_1(\alpha)][F_1(\alpha):F_1] = [K_1:F_1]$ such maps.

Moreover, if $m_{\alpha,F_1}$ does not split into distinct linear factors in $K_2[X]$ then $r < \deg m_{\alpha,F_1}$ and we have a strict inequality. Conversely if every $m_{\alpha,F_1}$ does split into distinct linear factors then $r = \deg m_{\alpha,F_1}$. Also every $\phi_i(m_{\alpha',F_1}(\alpha))$ with $\alpha' \in A$ splits into distinct linear factors in $K_2[X]$ since they are factors of $\phi(m_{\alpha',F_1})$. Hence by induction the number of extensions of each $\phi_i$ is exactly $[K_1:F_1(\alpha)]$ and we have equality.

There are therefore two ways in which we may have fewer that $[K_1:F_1]$ maps in Lemma 1. The first is if $K_2$ is not “big enough”. In this case some of the $m_{\alpha,F_1}$ may not split. The other is that the $m_{\alpha,F_1}$ may split, but some of the roots may be multiple roots. This motivates the following definitions.

Definition An irreducible polynomial $f \in F[X]$ is called separable if it has no multiple roots in any of its extensions. An element $\alpha \in K$ is called separable over $F$ if it is algebraic over $F$ and $m_{\alpha,F}$ is separable in $F[X]$. An extension $K/F$ is separable if every $\alpha \in K$ is separable over $F$.

Definition The separable degree $[K:F]_s$ of an algebraic extension $K/F$ is the number of maps $\phi: K \to M$ which fix $F$, where $M/F$ is any “sufficiently large” extension.

Here “sufficiently large” means that all the $m_{\alpha,F}$’s in Lemma 1 split in $K_2 = M$. In this case the separable degree will be independent of $M$. It is enough if $M$ is a normal closure of $K/F$. You can also use $M = F$, the algebraic closure of $F$.

Corollary 2 If $K/F$ is finite then $[K:F]_s \leq [K:F]$ with equality iff $K/F$ is separable.

Proof. Immediate from Lemma 1 taking $A = K$. 

Example Let $K = \mathbb{F}_p(t)$ and $F = \mathbb{F}_p(t^p) \subseteq K$ where $t$ is a transcendental element over $\mathbb{F}_p$. Then $K$ is obtained from $F$ by adjoining a root of $f(X) = X^p - t^p$. In $K[X]$, $f(X)$ splits as $f(X) = (X - t)^r$. The only non-trivial monic factors of $f$ in $K[X]$ are therefore of the form $(X - t)^r$, $0 < r < p$, and it is clear that these do not lie in $F[X]$ (consider the constant term). Hence $f$ is irreducible in $F[X]$ and so $f$, $t$, and $K$ are inseparable over $F$. 


In fact the above example is typical as the following lemma shows.

**Lemma 3** If $f \in F[X]$ is irreducible then the following are equivalent:

(a) $f$ is inseparable,

(b) $f' = 0$ where $f'$ is the formal derivative of $f$.

(c) char $F = p > 0$ and $f(X) = g(X^p)$ for some $g \in F[X]$.

**Proof.** Write $f = (X - \alpha)h(X)$ in some sfe. Then $f' = (X - \alpha)h' + 1.h$. In particular $f'(\alpha) = h(\alpha)$. If $\alpha$ is a multiple root of $f$ then $f'(\alpha) = h(\alpha) = 0$. But without loss of generality we can assume $f = m_\alpha$. Now since deg $f' < $ deg $f$ we have $f' = 0$. Conversely, if $\alpha$ is not a multiple root then $f'(\alpha) = h(\alpha) \neq 0$, so $f' \neq 0$. This proves (a) $\iff$ (b). The equivalence (b) $\iff$ (c) is immediate since if $f = \sum a_nX^n$ then $f' = \sum na_nX^{n-1}$. Hence $f' = 0$ iff $na_n = 0$ for all $n$. If char $F = 0$ then $f$ is a constant (contradicting the assumption that $f$ is irreducible). If char $F = p$ then $a_n = 0$ for all $p / |n$. Hence $f(X) = g(X^p)$. Conversely if $f(X) = g(X^p)$ and char $F = p$ then $f' = 0$.

**Definition** A field $F$ is called perfect if every algebraic extension $K/F$ is separable.

**Lemma 4** $F$ is perfect iff either (a) char $F = 0$, or (b) char $F = p > 0$ and every element of $F$ has a $p$th root in $F$.

**Proof.** If $F$ is perfect and char $F = p > 0$, consider the polynomial $X^p - a$ for $a \in F$. In a sfe $K/F$ this polynomial factors as $(X - b)^p$ where $b^p = a$. If $K/F$ is separable then $X^p - a$ cannot be irreducible in $F[X]$. Hence $f$ factors and one of the factors must be $(X - b)^i$ for some $0 < i < p$ (using unique factorization in $K[X]$). Hence $X^i - ibX^{i-1} + \cdots \in F[X]$. Hence $ib \in F$ and since $0 < i < p$, $b \in F$. Thus $a$ has a $p$th root in $F$.

If char $F = 0$ then and algebraic $K/F$ is separable. Assume char $F = p > 0$ and every element in $F$ has a $p$th root. If $\alpha$ is not separable over $F$ then the minimal polynomial of $\alpha$ is $f(X) = g(X^p)$ for some $g = \sum g_iX^i \in F[X]$. Let $h(X) = \sum g_i^{1/p}X^i$, where $g_i^{1/p}$ is any $p$th root of $g_i$ in $F$. Then $h(X)^p = (\sum g_i^{1/p}X^i)^p = \sum g_iX^{pi} = g(X^p) = f(X)$. Hence $f$ is not irreducible and cannot be the minimal polynomial of $\alpha$. Hence every algebraic $K/F$ is separable.

**Note:** If $K/F$ is an algebraic extension and char $F = 0$ then $K/F$ is automatically separable. Hence separability is only an issue in characteristic $p > 0$.

**Exercises**

1. Show that if char $F = p$ then the map $\phi: F \to F$ given by $\phi(a) = a^p$ is a homomorphism. Deduce that $F$ is perfect iff either char $F = 0$ or $\phi$ is an isomorphism. [\(\phi\) is called the Frobenius map.]

2. Show that if $F$ is finite then $\phi$ is an isomorphism. Deduce that all finite fields are perfect.
**Definition** Let $K/F$ be an arbitrary field extension, then the **Galois group** of $K/F$ is the group $\text{Gal}(K/F) = \{ \phi : K \to K : \phi|_F = 1, \phi \text{ is isomorphism} \}$, with the group operation given by composition.

**Definition** Let $K$ be a field and $G$ a group of ring (field) automorphisms of $K$. The **fixed field** of $G$ is $K^G = \{ \alpha \in K : \forall g \in G : g(\alpha) = \alpha \}$.

Note that $K^G$ is indeed a subfield of $K$. [Proof: $g(1) = 1$, so $1 \in K^G$. If $\alpha, \beta \in K^G$ then $g(\alpha - \beta) = g(\alpha) - g(\beta) = \alpha - \beta$, so $\alpha - \beta \in K^G$, similarly for $\alpha\beta, 1/\alpha$.]

**Note 1:** For any $K/F$ we have $F \subseteq K^{\text{Gal}(K/F)}$ and $G \subseteq \text{Gal}(K/K^G)$.

**Note 2:** If $K/F$ is Galois then $F \subseteq K^{\text{Gal}(K/F)} \subseteq K^G = F$. Thus without loss of generality we can assume $G = \text{Gal}(K/F)$ in the definition of Galois extension.

**Examples**

1. $\text{Gal}(\mathbb{C}/\mathbb{R}) = \{1, c\}$, where $c$ is complex conjugation. Now $\mathbb{C}^{\{1,c\}} = \{\alpha \in \mathbb{C} : \bar{\alpha} = \alpha \} = \mathbb{R}$. Hence $\mathbb{C}/\mathbb{R}$ is Galois.

2. If $\phi \in \text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ then $\phi(\sqrt{2})^3 = \phi(2) = 2$. Hence $\phi(\sqrt{2})$ is a root of $X^3 - 2 = 0$ in $\mathbb{Q}(\sqrt{2})$. But there is only one root $\sqrt{2}$, so $\phi(\sqrt{2}) = \sqrt{2}$. Since $\sqrt{2}$ generates $\mathbb{Q}(\sqrt{2})$, $\phi = 1$ and $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1\}$. Now $\mathbb{Q}(\sqrt{2})^{\{1\}} = \mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}$, so $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is not Galois.

3. If $\phi \in \text{Gal}(\mathbb{F}_p(t)/\mathbb{F}_p(t^p))$ then $\phi(t)^p = \phi(t^p) = t^p$. Thus $\phi(t)$ is a root of $X^p - t^p = (X - t)^p = 0$, so $\phi(t) = t$. Since $t$ generates $\mathbb{F}_p(t)$, $\phi = 1$ and $\text{Gal}(\mathbb{F}_p(t)/\mathbb{F}_p(t^p)) = \{1\}$. Now $\mathbb{F}_p(t)^{\{1\}} = \mathbb{F}_p(t) \neq \mathbb{F}_p(t^p)$, so $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ is not Galois.

**Theorem 1** $K/F$ is Galois if and only if it is both normal and separable.

**Proof.** The definitions of Galois, normal, and separable all require $K/F$ to be algebraic, so we can assume this. Assume first that $K/F$ is normal and separable. We know that $F \subseteq K^{\text{Gal}(K/F)}$, so it enough to show that for every $\alpha \in K$, $\alpha \notin F$, there exists a $\phi \in \text{Gal}(K/F)$ with $\phi(\alpha) \neq \alpha$. Since $K/F$ is normal, $m_{\alpha,F}$ splits in $K[X]$. Since $K/F$ is separable, $m_{\alpha,F}$ has distinct roots in $K$. Since $\alpha \notin F$, $\deg m_{\alpha,F} > 1$. Hence there is a $\beta \in K$ with $m_{\alpha,F}(\beta) = 0, \beta \neq \alpha$. By Artin’s extension theorem, there exists $\phi : F(\alpha) \to F(\beta)$ fixing $F$ with $\phi(\alpha) = \beta$. Since $K/F$ is normal, $K$ is the sfe of some $F \subseteq F[X]$ over $F$. Hence $K$ is a sfe of $F$ over either $F(\alpha)$ or $F(\beta)$. By the proof of the uniqueness of the sfe, there exists an isomorphism $\phi : K \to K$ that agrees with $\phi$ on $F(\alpha)$. This $\tilde{\phi}$ is an element of $\text{Gal}(K/F)$ which does not fix $\alpha$.

Now assume $K/F$ is Galois with $F = K^G$. For any $\alpha \in K$ let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r$ be the distinct values of $g(\alpha)$ as $g$ runs over $\text{Gal}(K/F)$. Note that there are only finitely many such values (even in $\text{Gal}(K/F)$ is infinite) since each $\alpha_i$ is a root of $m_{\alpha,F}$. Indeed, $r \leq \deg m_{\alpha,F}$. Consider the polynomial $f(X) = \prod_{i=1}^r (X - \alpha_i)$. Each $g \in G$ is injective on $K$ and if $\alpha_i = h(\alpha)$ then $g(\alpha_i) = (gh)(\alpha) = \alpha_j$ for some $j$. Hence $g$ permutes the $\alpha_i$’s and so $g(f(X)) = f(X)$. Thus
f \in K^G[X] = F[X]. But f(\alpha) = 0, so m_{\alpha,F} \mid f. Therefore m_{\alpha,F} splits into distinct linear factors in K[X]. Since this holds for any \alpha \in K, K/F is both normal and separable. \qed

**Note:** The first part of the proof of Theorem 1 shows that if K/F is Galois and \alpha \in K then Gal(K/F) permutes the roots of m_{\alpha,F} transitively, i.e., for any other root \beta there exists g \in Gal(K/F) with g(\alpha) = \beta.

**Theorem 2** If G is a finite group of automorphisms of K then [K:K^G] = |G| and G = Gal(K/K^G).

**Proof.** Assume first that [K:K^G] > |G| = n. Let \alpha_1, \ldots, \alpha_m, m > n, be a subset of K, linearly independent over K^G and let G = \{g_1, \ldots, g_n\}. Consider the system of linear equations

\[
g_j(\alpha_1)x_1 + \cdots + g_j(\alpha_m)x_m = 0, \quad j = 1, \ldots, n. \tag{1}
\]

There are n equations in m > n unknowns x_i. Hence there is a non-trivial solution with x_i \in K. Pick a non-trivial solution with the least number of non-zero x_i. Without loss of generality assume x_1, \ldots, x_r \neq 0 and x_{r+1}, \ldots, x_m = 0. Let g \in G and apply g to each of the equations above. Then

\[
g g_j(\alpha_1)g(x_1) + \cdots + g g_j(\alpha_r)g(x_r) = 0, \quad j = 1, \ldots, n. \tag{2}
\]

As j varies, gg_j runs over all the elements of G. Hence

\[
g_j(\alpha_1)g(x_1) + \cdots + g_j(\alpha_r)g(x_r) = 0, \quad j = 1, \ldots, n. \tag{3}
\]

Multiplying (2) by g(x_r) and (3) by x_r and subtracting gives

\[
\sum_{i=1}^r g_j(\alpha_i)(x_i g(x_r) - x_r g(x_i)) = 0.
\]

However the i = r term vanishes, so we get a solution to (1) with fewer non-zero x_i's. The only way in which this is possible is if all the coefficients x_i g(x_r) - x_r g(x_i) are zero. But then x_i/x_r = g(x_i/x_r) for all g \in G. Hence y_i = x_i/x_r \in K^G. Dividing through by x_r and setting g_j = 1 in (1) gives

\[
\alpha_1 y_1 + \cdots + \alpha_r y_r = 0
\]

with y_i \in K^G all non-zero. This contradicts the linear independence of the \alpha_i's. Hence [K:K^G] \leq |G|.

For any extension K/F, every element of Gal(K/F) is a map K \to K which fixes F, hence gives a map K \to M fixing F for any M/K. Thus |Gal(K/F)| \leq |K:F|. But [K:F] \leq [K:F], so

|Gal(K/K^G)| \leq [K:K^G] \leq |K:F| \leq |G|.

But G \subseteq Gal(K/K^G), so G = Gal(K/K^G) and |G| = [K:K^G]. \qed

**Exercises**

1. Show that Q(\sqrt[3]{2}, \sqrt[3]{3})/Q is Galois and Gal(Q(\sqrt[3]{2}, \sqrt[3]{3})/Q) \cong S_3. [Hint: consider the action of an automorphism on the roots of X^3 - 2 = 0].

2. For each subgroup G \leq Gal(Q(\sqrt[3]{2}, \sqrt[3]{3})/Q) identify the fixed field Q(\sqrt[3]{2}, \sqrt[3]{3})^H.

3. Show that if K/F is finite and separable then the normal closure M/F of K/F is finite and Galois.
Theorem (Fundamental Theorem of Galois Theory)
Assume \( K/F \) is a finite Galois extension, then there exists a bijection
\[
\{ \text{subgroups } H \leq \text{Gal}(K/F) \} \leftrightarrow \{ \text{subfields } L \subseteq K : K/L/F \} \\
H \rightarrow K^H \\
\text{Gal}(K/L) \leftrightarrow L
\]
Proof. Since \( |\text{Gal}(K/F)| \leq [K : F] \), \( \text{Gal}(K/F) \) is finite. We shall show the two maps given are inverse to each other. Starting with \( H \leq \text{Gal}(K/F) \) we get \( H \rightarrow K^H \rightarrow \text{Gal}(K/K^H) \). Now \( H \) is finite so \( H = \text{Gal}(K/K^H) \). Starting with \( L \subseteq K \), we get \( L \rightarrow \text{Gal}(K/L) \rightarrow K^{\text{Gal}(K/L)} \). However, \( K/L \) is both normal and separable (since \( K/F \) is), so \( K/L \) is Galois and \( L = K^{\text{Gal}(K/L)} \). Thus these maps are inverse to one another and we have a bijection. \( \square \)

Definition  The join or compositum \( L_1L_2 \) of two subfields \( L_1 \) and \( L_2 \) of a field \( K \) is the smallest field containing them both. I.e., \( L_1L_2 = L_1(L_2) = L_2(L_1) \).

Warning: It is possible that \( L_2 \cong L_3 \) but \( L_1L_2 \not\cong L_1L_3 \). Hence you should always specify \( L_1 \) and \( L_2 \) as subfields of a specific field \( K \). It is not enough just to define \( L_1 \) and \( L_2 \) up to isomorphism.

Corollary  Let \( K/F \) be a finite Galois extension with \( \text{Gal}(K/F) = G \). Let \( H_i \leq G \) and let \( L_i \subseteq K \) be the subfields corresponding to \( H_i \). Then
\begin{itemize}
  \item[(a)] \( H_1 \leq H_2 \) iff \( L_1 \supseteq L_2 \) and in this case \( [H_2 : H_1] = [L_1 : L_2] \),
  \item[(b)] \( H_1 \cap H_2 \) corresponds to \( L_1 \cap L_2 \),
  \item[(c)] \( \langle H_1 \cup H_2 \rangle \) corresponds to \( L_1 \cap L_2 \),
  \item[(d)] if \( g \in G \) then \( gHg^{-1} \) corresponds to \( g(L) \),
  \item[(e)] \( H_1 \leq H_2 \iff L_2/L_1 \) is Galois \( \iff L_2/L_1 \) is normal, and in this case \( \text{Gal}(L_1/L_2) \cong H_2/H_1 \).
\end{itemize}
Proof.
\begin{itemize}
  \item[(a)] If \( H_1 \leq H_2 \), then \( L_1 = K^{H_1} \supseteq K^{H_2} = L_2 \).
  \item[(b)] If \( L_1 \supseteq L_2 \), then \( H_1 = \text{Gal}(K/L_1) \leq \text{Gal}(K/L_2) = H_2 \).
  \item[(c)] \( \langle H_1 \cup H_2 \rangle \) is the largest subgroup of \( G \) that contains both \( H_1 \) and \( H_2 \). This corresponds to the largest subfield of \( K \) that contains both \( L_1 \) and \( L_2 \), but this is just \( L_1L_2 \).
  \item[(d)] Any element of \( g(L) \) is of the form \( g(\alpha) \) with \( \alpha \in L \). But if \( ghg^{-1} \in gHg^{-1} \) then \( h \) fixes \( \alpha \) and so \( ghg^{-1}(g(\alpha)) = g(h(\alpha)) = g(\alpha) \). Thus \( g(\alpha) \) is fixed by \( gHg^{-1} \), \( g(L) \subseteq K^{gHg^{-1}} \). But \( g \) is an automorphism of \( K \), so \( [K : g(L)] = [g(K) : g(L)] = [K : L] \). Also \( [K : L] = |H| = |gHg^{-1}| = [K : K^{gHg^{-1}}] \). Hence \( g(L) = K^{gHg^{-1}} \).
  \item[(e)] If \( H_1 \leq H_2 \) then \( gH_1g^{-1} = H_1 \), so \( g(L_1) = L_1 \) for all \( g \in H_2 = \text{Gal}(K/L_2) \). Hence \( g|_{L_1} \in \text{Gal}(L_1/L_2) \). Thus we have a map \( \phi: \text{Gal}(K/L_2) \rightarrow \text{Gal}(L_1/L_2) \) which maps \( g \mapsto g|_{L_1} \).
   This is clearly a group homomorphism with kernel equal to \( \text{Gal}(K/L_1) \). But \( L_2 \subseteq L_1^{\text{Gal}(L_1/L_2)} \subseteq \)}
$L_1^{\text{Im} \phi} \subseteq K^\text{Gal}(K/L_2) = L_2$, so $L_1/L_2$ is Galois. If $L_1/L_2$ Galois then $L_1/L_2$ normal, so we now prove $L_1/L_2$ normal implies $H_1 \trianglelefteq H_2$. If $L_1/L_2$ is normal and $g \in H_2$, then $g(L_1)$ must have the same image in $K$ as $1(L_1) = L_1$. Hence $g(L_1) = L_1$ and $gH_1g^{-1} = H_1$. Thus $H_1 \leq H_2$. Finally $H_2/H_1 = H_2/\text{Ker} \phi \cong \text{Im} \phi$ is a subgroup of $\text{Gal}(L_1/L_2)$, but $[H_2:H_1] = [L_1:L_2] = |\text{Gal}(L_1/L_2)|$, so the image of $\phi$ is $\text{Gal}(L_1/L_2)$ and $\text{Gal}(L_1/L_2) \cong H_2/H_1$. 

**Lemma 1** If $K/F$ is the sfe for $f \in F[X]$ then $\text{Gal}(K/F)$ is isomorphic to a subgroup of the symmetric group $S_R$ where $R$ is the set of roots of $f$ in $K$.

**Proof.** Map $\text{Gal}(K/F) \to S_R$ by restricting $\phi \in \text{Gal}(K/F)$ to $R \subseteq K$. The image is a permutation since $\phi$ is injective and maps the finite set $R$ to $R$. The map is a group homomorphism since the group operation on each side is the same — composition of functions. If the image in $S_R$ is the identity then $\phi$ fixes $R$ and $F$, so fixes $F(R) = K$ and so $\phi = 1$. Hence the map $\text{Gal}(K/F) \to S_R$ is injective and $\text{Gal}(K/F)$ is isomorphic to the image of this map in $S_R$. 

**Example** Consider $\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}$ which is the sfe of $x^4 - 2$. Let $G = \text{Gal}(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q})$. By Artin’s extension Theorem there exists a $\sigma \in G$ with $\sigma(\sqrt{2}) = i\sqrt{2}$. There is also $c \in G$ with $c =$ complex conjugation. We do not know what $\sigma(i)$ is, but if $\sigma(i) = -i$ then $\sigma c(i) = i$ and $\sigma c(\sqrt{2}) = \sqrt{2}$. Hence by replacing $\sigma$ with $\sigma c$ if necessary we may assume $\sigma(i) = i$. Let the four roots of $X^4 - 2$ be

$$\alpha_1 = \sqrt{2}, \quad \alpha_2 = i\sqrt{2}, \quad \alpha_3 = -\sqrt{2}, \quad \alpha_4 = -i\sqrt{2}.$$ 

Then $\sigma$ acts as the permutation $(1234)$ and $c$ acts as the permutation $(24)$ on the roots. The subgroup of $S_4$ generated by these is $D_4$ which is of order 8. But $|G| = [\mathbb{Q}(\sqrt{2},i):\mathbb{Q}] = 8$, so $G = \langle \sigma, c \rangle \cong D_4$. The subgroups of $G$ and their corresponding subfields are:

![Diagram](image)

In order to apply Galois theory we need a finite Galois extension. The following Lemma is therefore extremely useful.

**Lemma 2** If $K/F$ is finite and separable and if $M$ is the normal closure of $K/F$ then $M/F$ is finite and Galois.

**Proof.** If $K/F$ is finite and separable then $K = F(\alpha_1, \ldots, \alpha_r)$ where each $\alpha_i$ is separable over $F$. Then $M$ is the sfe for $F = \{m_{\alpha_1,F}, \ldots, m_{\alpha_r,F}\}$ which is a finite set of separable polynomials. Hence $M$ is normal (since it is a sfe), separable (since it is generated by the roots of the $m_{\alpha_i,F}$ which are all separable), and finite (since it is the sfe of a finite set of polynomials). 


Definition If $F$ is a field of characteristic $p$, then the map $\phi: F \to F$ given by $\phi(a) = a^p$ is called the Frobenius map.

Lemma 1 The Frobenius map is a ring homomorphism from $F$ to $F$.

Proof. If $a, b \in F$ then $\phi(a + b) = (a + b)^p = a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p-1}ab^{p-1} + b^p$. However, for $0 < i < p$ the binomial coefficient $\binom{p}{i} = p!/i!(p-i)!$ is divisible by $p$ since $p \mid p!$ but $p \not\mid i!(p-i)!$. Hence $\phi(a + b) = a^p + b^p = \phi(a) + \phi(b)$. Also $\phi(1) = 1$ and $\phi(ab) = (ab)^p = a^pb^p = \phi(a)\phi(b)$. Thus $\phi$ is a ring homomorphism.

Note: The Frobenius map is always injective, but it need not be surjective. For example, take $F = \mathbb{F}_p(t)$ where $t$ is transcendental over $\mathbb{F}_p$.

Theorem 2 For all primes $p$ and all $n \geq 1$ there exists a field $\mathbb{F}_{p^n}$ with $p^n$ elements which is the sfe of $X^{p^n} - X$ over $\mathbb{F}_p$. Conversely every finite field is isomorphic to some $\mathbb{F}_{p^n}$.

Proof. Let $K$ be the sfe of $f(X) = X^{p^n} - X$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Then $K$ is finite and the Frobenius map $\phi$ is therefore an automorphism of $K$. Let $G$ be the cyclic group of automorphisms of $K$ generated by $\phi^n$. Then $K^G = \{ \alpha : \phi^n(\alpha) = \alpha \} = \{ \alpha : \alpha^{p^n} = \alpha \}$ is just the set of roots of $f$ in $K$. But $K^G$ is a subfield of $K$ containing $\mathbb{F}_p$ and all the roots of $f$. Hence $K = K^G = \{ \alpha : f(\alpha) = 0 \}$. If $f$ has a multiple root $\alpha \in K$ then $f'(\alpha) = 0$. But $f' = -1$, so $f$ has no multiple roots. Since $f$ splits in $K$, there are exactly $p^n$ roots of $f$ in $K$, and $|K| = p^n$.

Now assume $K$ is some finite field. The characteristic of $K$ cannot be zero, since otherwise $K$ would contain $\mathbb{Q}$ which is infinite. Assume char $K = p$. Then $\mathbb{F}_p \subseteq K$ and so $K/\mathbb{F}_p$ is a field extension. The extension is clearly finite since one cannot have a basis for $K/F$ with more than $|K|$ elements. If $[K: \mathbb{F}_p] = n$ then $K \cong \mathbb{F}_{p^n}$ as a vector space, so $|K| = p^n$. Any $\alpha \in K$ is either zero, or in $K^\times$ which is a group of order $p^{n-1} - 1$. Hence either $\alpha = 0$ or $\alpha^{p^{n-1}} = 1$. Thus every $\alpha \in K$ is a root of $f(X) = X^{p^n} - X$. Since there are at most $p^n$ roots of $f$ in $K$ and $|K| = p^n$, $f$ splits in $K$. Thus $K$ contains a sfe of $f$ over $\mathbb{F}_p$. But since $K$ consists of the roots of $f$, $K$ must be equal to a sfe of $f$ over $\mathbb{F}_p$. Since any two sfe’s are isomorphic, $K \cong \mathbb{F}_{p^n}$.

Theorem 3 Any finite extension $K/F$ of a finite field $F$ is Galois. The Galois group is cyclic and is generated by a power of the Frobenius map.

Proof. Since $|F| < \infty$ and $|K:F| < \infty$, we have $|K| = |F|^{|K:F|} < \infty$. Assume $K = \mathbb{F}_{p^n}$ and let $G$ be the cyclic group of automorphisms generated by the Frobenius map $\phi$. The fixed field $K^G = \{ \alpha : \phi^n(\alpha) = \alpha \}$ is just the set of roots of the polynomial $X^{p^n} - X = 0$. But there are at most $p^n$ roots, and $\phi$ fixes $\mathbb{F}_p$. Therefore $K^G = \mathbb{F}_p$. Hence $K/\mathbb{F}_p$ is Galois and Gal($K/\mathbb{F}_p$) = $G$ is cyclic generated by Frobenius.

Now if $K/F$ then $\mathbb{F}_p \subseteq F \subseteq K$, so by the Fundamental theorem of Galois theory, $F = K^H$ for some $H \leq G$. Thus $K/F$ is Galois with Galois group Gal($K/F$) = $H$. Now $H$ is a subgroup of a cyclic group $G$, so is cyclic. It is generated by some element, which is a power of $\phi$.

Note: If $K = \mathbb{F}_{p^n}$ then the Galois group is cyclic of order $n$. The subgroups are cyclic of order $m$ for some $m | n$ and are generated by $\phi^{n/m}$. The fixed field of $\phi^{n/m}$ is just $\mathbb{F}_{p^{n/m}}$. Hence the subfields of $\mathbb{F}_{p^n}$ are precisely the $\mathbb{F}_{p^r}$ for all $r | n$. Spring 2003
Corollary 4  For each $n$ there exists some irreducible polynomial of degree $n$ in $\mathbb{F}_p[X]$. Furthermore $X^{pn} - X$ is the product of all monic irreducible polynomials of degree $d | n$.

Proof. The group $\mathbb{F}_p^\times$ is cyclic, generated by $\alpha$ say. Then $\mathbb{F}_p^n = \mathbb{F}_p(\alpha)$ and the minimal polynomial $m_{\alpha, \mathbb{F}_p}$ is irreducible of degree $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [\mathbb{F}_{pn} : \mathbb{F}_p] = n$.

Write $X^{pn} - X = \prod f_i$ where $f_i$ are irreducible monic polynomials in $\mathbb{F}_p[X]$. If $\alpha$ is a root of $f_i$ in the sfe $\mathbb{F}_{pn}$, then $\mathbb{F}_p(\alpha)$ is a subfield of $\mathbb{F}_{pn}$. Hence $\mathbb{F}_p(\alpha) = \mathbb{F}_{pd}$ for some $d | n$ and $f_i = m_{\alpha, \mathbb{F}_p}$ has degree $[\mathbb{F}_{pd} : \mathbb{F}_p] = d$. Conversely if $f$ is an irreducible polynomial of degree $d | n$, and $\alpha$ is a root of $f$ in some extension, then $\mathbb{F}_p(\alpha)$ is isomorphic to $\mathbb{F}_{pd}$. But every element of $\mathbb{F}_{pd}$ is a roots of $X^{pd} - X | X^{pn} - X$. Hence $\alpha$ is a root of $X^{pn} - X$. Thus $f | X^{pn} - X$. Since $X^{pn} - X$ has no multiple roots, it cannot be divisible by $f^2$. Hence $X^{pn} - X$ is precisely the product of monic irreducible polynomials of degree $d | n$. \qed

Lemma 5  If $f \in \mathbb{F}_p[X]$ and $f = f_1 f_2 \ldots f_r$ where $f_i \in \mathbb{F}_p[X]$ are distinct irreducibles, then the sfe for $f$ over $\mathbb{F}_p$ is $\mathbb{F}_{p^r}$ where $r = \text{lcm}\{\deg f_i\}$. The Frobenius map $\phi$ acts on the roots of $f$ as a permutation of cycle type $(\deg f_1)(\deg f_2) \ldots (\deg f_r)$ in $S_{\deg f}$ permuting the roots of each $f_i$ cyclically.

Proof. Let $K$ be the sfe for $f$. The Galois group $G = \text{Gal}(K/\mathbb{F}_p)$ permutes the roots of each $f_i$ transitively and is also cyclic, generated by the Frobenius map $\phi$. The only way this can happen is if $\phi$ permutes the roots of $f_i$ cyclically. Finally, if $K = \mathbb{F}_{p^r}$ then $r = [K : \mathbb{F}_p] = |G| = \text{order of } \phi$, which is lcm\{\deg f_i\}. \qed

Theorem 6  If $f = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$, $p$ is a prime with $p \not| a_n$, and the reduction $\bar{f}$ of $f$ mod $p$ is a product of distinct irreducible polynomials in $\mathbb{F}_p[X]$, $\bar{f} = f_1 \ldots f_r$, then $\text{Gal}(f/\mathbb{Q})$ contains an automorphism which acts on the roots of $f$ as a permutation with cycle type $(\deg f_1)(\deg f_2) \ldots (\deg f_r)$.

The proof of this result is rather technical, so I will not include it here.

Exercises

1. How many irreducible polynomials of degree 4 are there in $\mathbb{F}_2[X]$. [Hint: Corollary 4.]
2. List all irreducible polynomials of degree 4 in $\mathbb{F}_2[X]$.
3. Find the Galois group of $X^5 + X^4 + 1$ over $\mathbb{F}_2[X]$.
4. Find the Galois group of $X^4 + 10X^3 - 5X^2 - 5X + 30$ over $\mathbb{Q}[X]$.
   [Hint: Use Theorem 6 with $p = 2$ and 3.]
Definition A primitive nth root of 1 is an element $\zeta_n \in K$ with order n in $K^\times$, i.e., $\zeta_n^n = 1$ but $\zeta_n^r \neq 1$ for $0 < r < n$.

Lemma 1 If $K/F$ is a sfe for $X^n - 1$ and char $F \nmid n$ then the roots of $X^n - 1$ in $K$ are \{1, $\zeta_n, \ldots, \zeta_{n-1}^n$\} where $\zeta_n \in K$ is a primitive nth root of 1. Also $K = F(\zeta_n)$ and $K/F$ is Galois with $Gal(K/F) \leq (\mathbb{Z}/n\mathbb{Z})^\times$ where $(\mathbb{Z}/n\mathbb{Z})^\times = \{r \mod n : \text{gcd}(r, n) = 1\}$ is the group of units of $\mathbb{Z}/n\mathbb{Z}$ under multiplication.

Proof. Let $A = \{\alpha \in K : \alpha^n = 1\}$. Then $A$ is a subgroup of $K^\times$. If $\alpha$ is a multiple root of $f(X) = X^n - 1$ then $f'(\alpha) = n\alpha^{n-1} = 0$. But $\alpha \neq 0$ and char $F \nmid n$, so this is impossible. Hence $|A| = n$. Since any finite subgroup of $K^\times$ is cyclic, $A = \{1, \zeta_n, \ldots, \zeta_{n-1}^n\}$ for some $\zeta_n$ which is then a primitive nth root of 1. Now $K = F(A) = F(\zeta_n)$ is normal and separable over $F$, so $K/F$ is Galois. If $\sigma \in Gal(K/F)$ then $\sigma(\zeta_n) = \zeta_n^s$ for some r which is uniquely determined mod $n$. But $\zeta_n^s$ must also have order $n$ in $K^\times$ since $\sigma$ is an automorphism. Hence gcd($r, n$) = 1. Thus we have a map $Gal(K/F) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ sending $\sigma$ to $r \mod n$. This map is a group homomorphism since if $\sigma(\zeta_n) = \zeta_n^s$ and $\tau(\zeta_n) = \zeta_n^t$ then $\sigma \tau(\zeta_n) = \sigma(\tau(\zeta_n)) = \sigma(\zeta_n^s) = \zeta_n^{st}$ and $\sigma \tau$ is mapped to $rs$. This map is injective since $K = F(\zeta_n)$, so if $\sigma(\zeta_n) = \zeta_n^s$ then $\sigma = 1$. Hence $Gal(K/F)$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.

Note that it is not always the case that $Gal(K/F) = (\mathbb{Z}/n\mathbb{Z})^\times$. For example, $F$ may already contain $\zeta_n$ in which case $K = F$ and $Gal(K/F) = \{1\}$.

Definition Let char $K = 0$ and let $\zeta_n \in K$ be a primitive nth root of 1. Define $\Phi_n(X) = \prod_{\zeta \in K} (X - \zeta)$.

Lemma 2 For $n > 0$, $X^n - 1 = \prod_{d|n} \Phi_d(X)$, and $\Phi_n(X)$ is an irreducible element of $\mathbb{Z}[X]$.

Proof. Note that $\Phi_n(X) = \prod_{\zeta} (X - \zeta)$ where the product runs over all primitive nth roots of 1. Also $\Phi_n(X) \in \mathbb{Q}(\zeta_n)[X]$ and for any $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, $\sigma(\Phi_n) = \Phi_n$ since $\sigma$ permutes the set of primitive nth roots of 1. Thus $\Phi_n \in \mathbb{Q}(\zeta_n)^{Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})}[X] = \mathbb{Q}[X]$.

For any $r$, $\zeta_n^s$ has order $d = n/\text{gcd}(r, n)$, so is a primitive dth root of 1 for some $d \mid n$. Conversely any primitive dth root of 1 is of the form $\zeta_n^s$ for some $r$ since it is a power of a fixed primitive dth root of 1, namely $\zeta_n^{n/d}$. Hence $X^n - 1 = \prod_r (X - \zeta_n^r) = \prod_{d|n} \prod_{s|d} (X - \zeta_n^s)$ where the second product is over all primitive dth roots of 1. Therefore $X^n - 1 = \prod_{d|n} \Phi_d(X)$. Now by induction we can assume $\Phi_d \in \mathbb{Z}[X]$ for all $d < n$. Hence both $X^n - 1$ and $\prod_{d|n, d<n} \Phi_d$ are monic (and hence primitive) elements of $\mathbb{Z}[X]$. Thus by Gauss’ Lemma $\Phi_n \in \mathbb{Z}[X]$. It remains to show that $\Phi_n$ is irreducible in $\mathbb{Z}[X]$.

Write $\Phi_n = fg$ where $f = m_{\zeta_n, \mathbb{Q}}$. Then by Gauss $f, g \in \mathbb{Z}[X]$. If $\Phi_n$ is not irreducible then deg $g > 0$ and $g(\zeta_n^r) = 0$ for some $r > 1$, $\text{gcd}(r, n) = 1$. Write $r$ as a product of (not necessarily distinct) primes $r = p_1 \ldots p_s$. By considering $\zeta_n^{p_1 \ldots p_i}$ for each $i = 0, \ldots, s$ there must be some $\alpha$ and prime $p \mid n$ such that $f(\alpha) = 0$ and $g(\alpha^p) = 0$. Hence $f = m_{\alpha, \mathbb{Q}}$ and $f(X) \mid g(X^p)$ in $\mathbb{Z}[X]$. Consider the reductions $\tilde{f}$ and $\tilde{g}$ of $f$ and $g$ mod $p$. Then $\tilde{f}(X) \mid \tilde{g}(X^p) = (\tilde{g}(X))^p$. Then any root $\beta$ of $\tilde{f}$ is also a root of $\tilde{g}$, so is a multiple root of $\Phi_n = \tilde{f}\tilde{g}$. Hence $\beta$ is a multiple root of $X^n - 1 = \Phi_n \ldots \Phi_1$. But then $\beta$ is a root of the derivative $nX^{n-1}$ and since $p \nmid n$ this implies $\beta = 0$ which is not a root of $X^n - 1$. Hence $\Phi_n$ is irreducible in $\mathbb{Q}[X]$. □
Corollary 3 If \( \zeta_n \) is a primitive \( n \)th root of 1 then \( \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times \).

Proof. \( |\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = |\mathbb{Q}(\zeta_n) : \mathbb{Q}| = \deg m_{\zeta_n, \mathbb{Q}} = \deg \Phi_n = |\{ r \mod n : \gcd(r, n) = 1\}| = |(\mathbb{Z}/n\mathbb{Z})^\times| \). Since \( \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \leq (\mathbb{Z}/n\mathbb{Z})^\times \), the groups must be equal. \( \square \)

We now consider the equation \( X^n - a = 0 \) with \( a \neq 1 \).

Lemma 4 Assume \( F \) contains a primitive \( n \)th root of 1. If \( K \) is the subfield of \( X^n - a \) then \( \text{Gal}(K/F) \) is isomorphic to a subgroup of the cyclic group \( \mathbb{Z}/n\mathbb{Z} \). Conversely, if \( K/F \) is a Galois extension with \( \text{Gal}(K/F) = \mathbb{Z}/n\mathbb{Z} \), then \( K = F(\alpha) \) for some \( \alpha \) with \( \alpha^n \in F \).

Proof. The roots of \( X^n - a \) are of the form \( \{ \zeta_n^i \alpha : 0 \leq i < n \} \) for some \( \alpha \in K \) with \( \alpha^n = a \). If \( \sigma \in \text{Gal}(K/F) \) then \( \sigma(\alpha) = \zeta_n^i \alpha \) for some \( i \in \mathbb{Z}/n\mathbb{Z} \). Since \( \zeta_n \in F \), \( \sigma(\zeta_n) = \zeta_n \). Thus if \( \tau(\alpha) = \zeta_n^i \alpha \) then \( \sigma \tau(\alpha) = \zeta_n^{i+j} \alpha \), so the map \( \text{Gal}(K/F) \to (\mathbb{Z}/n\mathbb{Z}, +) \) sending \( \sigma \) to \( i \mod n \) is a homomorphism. This map is injective since if \( \sigma(\alpha) = \zeta_n^0 \alpha = \alpha \) then \( \sigma \) fixes \( F \) and \( \alpha \), so fixes \( F(\alpha) = K \). Hence \( \text{Gal}(K/F) \) is isomorphic to a subgroup of \( \mathbb{Z}/n\mathbb{Z} \). Conversely, assume \( K/F \) is a Galois extension with \( \text{Gal}(K/F) = (\sigma) \), and \( \sigma \) of order \( n \). For \( \alpha \in K \) define \( \beta = \alpha + \sigma(\alpha) \zeta_n^{-1} + \cdots + \sigma^{n-1}(\alpha) \zeta_n^{-(n-1)} \).

Then \( \sigma(\beta) = \zeta_n \beta \). Hence \( \sigma(\beta^n) = \beta^n \) and so \( \beta^n \in K^{\text{Gal}(K/F)} = F \). It remains to prove that we can choose \( \alpha \) so that \( F(\beta) = K \). If \( \beta \neq 0 \) then \( \sigma^i(\beta) = \zeta_n^i \beta \) gives \( n \) distinct values as \( i \) varies from 0 to \( n - 1 \). Hence \( m_{\beta,F} \) has \( n \) distinct roots and \( [F(\beta):F] = \deg m_{\beta,F} \geq n = |\text{Gal}(K/F)| = [K:F] \) so \( F(\beta) = K \). The result now follows from the following Theorem with \( \sigma_i = \sigma_i^{i-1} \) and \( \lambda_i = \zeta_n^{i(i-1)} \).

Theorem (Dedekind Indepence Theorem) Suppose \( \sigma_1, \ldots, \sigma_n \) are distinct automorphisms of a field \( K \), then for any \( \lambda_1, \ldots, \lambda_n \in K \) not all zero, there is an \( \alpha \in K \) such that \( \sum_{i=1}^n \lambda_i \sigma_i(\alpha) \neq 0 \).

Proof. We shall prove the result by induction on \( n \). For \( n = 1 \) the result is clear. Assume \( n > 1 \) and suppose \( \sum \lambda_i \sigma_i(\alpha) = 0 \) for all \( \alpha \in K \). Since \( \sigma_1 \neq \sigma_2 \) there is an \( \beta \in K \) with \( \sigma_1(\beta) \neq \sigma_2(\beta) \). Then for all \( \alpha \in K \)

\[
\sum \lambda_i \sigma_i(\beta) \sigma_i(\alpha) = \sum \lambda_i \sigma_i(\alpha \beta) = 0
\]

\[
\sum \lambda_i \sigma_1(\beta) \sigma_i(\alpha) = \sigma_1(\beta) \sum \lambda_i \sigma_i(\alpha) = 0
\]

Subtracting we get \( \sum_{i=2}^n \lambda_i (\sigma_i(\beta) - \sigma_1(\beta)) \sigma_i(\alpha) = 0 \) since the terms for \( i = 1 \) cancel. Hence by induction \( \lambda_1 (\sigma_i(\beta) - \sigma_1(\beta)) = 0 \) for all \( i \), in particular \( \lambda_2 (\sigma_2(\beta) - \sigma_1(\beta)) = 0 \). But then \( \lambda_2 = 0 \). Repeating this argument for any pair \( (i,j) \) in place of \( (1,2) \) gives \( \lambda_j = 0 \) for all \( j \).

\( \square \)

Exercises

1. Calculate \( \Phi_n(X) \) for \( n = p \), a prime, and for \( n = 1, 6, 8, 12 \).
2. Show that \( |\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})| = 2 \) for all \( n > 2 \).
3. Show that the angle \( 2\pi/n \) is constructible iff \( |(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n) \), the Euler function, is a power of 2. [Hint: \( 2 \cos(2\pi/n) = \zeta_n + \zeta_n^{-1} \).] Characterize such \( n \).
4. Show that if \( \text{char} F \nmid n \) then the Galois group \( G \) of \( X^n - a \) over \( F \) has a normal subgroup \( H \) with \( H \) abelian and \( G/H \) cyclic. [In particular, \( G \) is solvable. Note we don’t assume \( \zeta_n \in F \).]
We shall assume throughout that \( \text{char } F = 0 \), \( f \in F[X] \), and \( K/F \) is a sfe for \( f \). Write the roots of \( f \) in \( K \) as \( \alpha_1, \ldots, \alpha_n \).

**Quadratics**

Let \( f(X) = aX^2 + bX + c \). In general \( \text{Gal}(K/F) \cong S_2 = C_2 \), and \( \zeta_2 = -1 \in F \), so \( K = F(\sqrt{d}) \) for some \( d \in F \). To find \( d \) we use the trick in Lemma 4 of the last section. \( \text{Gal}(K/F) = \langle \sigma \rangle \) where \( \sigma \) acts as the permutation \((12)\) on the roots. Let \( \beta = \alpha_1 + \zeta_2^{-1} \sigma(\alpha_1) = \alpha_1 - \alpha_2 \). Then \( \beta^2 \) is fixed by \( S_2 \). Thus \( \beta^2 \) can be written in terms of elementary symmetric functions of the roots, and hence in terms of the coefficients of \( f \). Indeed \( \beta^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = (-b/a)^2 - 4(c/a) = (b^2 - 4ac)/a^2 \). Using \( \alpha_1 + \alpha_2 = -b/a \) and \( \alpha_1 - \alpha_2 = \beta = \sqrt{b^2 - 4ac}/a \) we can now solve for \( \alpha_1, \alpha_2 \) to give the well known formula \( \alpha_i = (-b \pm \sqrt{b^2 - 4ac})/2a \). It can be checked that this formula also works when \( \text{Gal}(K/F) < S_2 \) (in which case \( \sqrt{d} \in F \)).

**Cubics**

Assume \( \zeta_3 \in F \) and \( \text{Gal}(K/F) \cong S_3 \). Then there is an intermediate field \( L \) with \( \text{Gal}(K/L) \cong A_3 = C_3 \) and \( \zeta_3 \in L \). Write

\[
\begin{align*}
z_0 &= \alpha_1 + \alpha_2 + \alpha_3 \\
z_1 &= \alpha_1 + \zeta_3 \alpha_2 + \zeta_3^2 \alpha_3 \\
z_2 &= \alpha_1 + \zeta_3^2 \alpha_2 + \zeta_3 \alpha_3
\end{align*}
\]

Then \( A_3 \) fixes \( z_1^3 \) and \( z_2^3 \) so \( z_1^3, z_2^3 \in L \). But the transposition \((23)\) swaps \( z_1^3 \) and \( z_2^3 \) so in general we do not expect \( z_1^3 \) or \( z_2^3 \) to lie in \( F \). Construct a new polynomial

\[
g(X) = (X - z_1^3)(X - z_2^3) = X^2 - (z_1^3 + z_2^3)X + z_1^3 z_2^3
\]

This polynomial is fixed by \( S_3 \) and so we can write its coefficients in terms of the coefficients of \( f \). Indeed, by “completing the cube” we can assume \( f(X) = X^3 + pX + q \), in which case \( g(X) = X^2 + 27qX - 27p^3 \) and \( z_0 = 0 \). Solving \( g(X) = 0 \) then gives \( z_1^3, z_2^3 \) as roots. Since we know \( z_0 \) we can now reconstruct the roots as

\[
\begin{align*}
\alpha_1 &= (z_0 + z_1 + z_2)/3, \\
\alpha_2 &= (z_0 + \zeta_3 z_1 + \zeta_3^2 z_2)/2, \\
\alpha_3 &= (z_0 + \zeta_3 z_1 + \zeta_3^2 z_2)/2.
\end{align*}
\]

As for the quadratics, these formula work even if \( \text{Gal}(K/F) < S_3 \).

**Quartics**

Assume \( \zeta_4 \in F \) and \( \text{Gal}(K/F) \cong S_4 \). By “completing the quartic” we can write \( f \) in the form \( f(X) = X^4 + pX^2 + qX + r \) so that \( \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0 \). There is an intermediate field \( L \) with \( \text{Gal}(K/L) = V \), the Klein group. Now \( V \leq S_4 \) and \( \text{Gal}(L/F) \cong S_4/V \cong S_3 \), so with some luck we can get \( L \) by splitting a cubic. Write

\[
\begin{align*}
y_1 &= (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = -(\alpha_1 + \alpha_2)^2 \\
y_2 &= (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) = -(\alpha_1 + \alpha_3)^2 \\
y_3 &= (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3) = -(\alpha_1 + \alpha_4)^2
\end{align*}
\]

Then \( y_i \) is fixed by \( V \) so \( y_i \in L \). The cubic

\[
g(X) = (X - y_1)(X - y_2)(X - y_3)
\]
is now fixed by $S_4$, so the coefficients of $g$ are polynomials in the coefficients of $f$. Indeed $g(X) = X^3 - 2pX^2 + (p^2 - 4r)X + q^2$. Finding the roots $y_1, y_2, y_3$ as above we can recover $\alpha_i = (\pm \sqrt{-y_1} \pm \sqrt{-y_2} \pm \sqrt{-y_3})/2$ for suitable choice of signs (signs chosen so that the product of the square root terms is $-q$). Once again, the formulae obtained work even when $\text{Gal}(K/F) < S_4$.

**General Case**

**Definition** An extension $K/F$ is a radical extension if $K = F(\alpha_1, \ldots, \alpha_n)$ and there exists integers $n_i > 0$ such that $\alpha_i^{n_i} \in F(\alpha_1, \ldots, \alpha_{i-1})$ for each $i$.

**Lemma 1** If $F \subseteq L_1, L_2 \subseteq K$ and $L_1/F$ and $L_2/F$ are radical, then so is the join $L_1L_2/F$.

*Proof.* Clear.

**Lemma 2** If $K/F$ is radical and $M/K$ is the normal closure of $K/F$ then $M/F$ is radical.

*Proof.* If $K/F$ is radical, then $g(K)/g(F) = g(K)/F$ is radical for each $g \in \text{Gal}(M/F)$. Hence the join $L$ of all the $g(K)$ is radical over $F$. But if $H = \text{Gal}(M/K)$ then $\text{Gal}(M/L) = \bigcap gHg^{-1}$. However, this is a normal subgroup of $\text{Gal}(M/F)$, so $L/F$ is normal and $L \supseteq K$. Thus $L = M$ is radical over $F$.

**Theorem 3** If $K/F$ is radical and normal then $\text{Gal}(K/F)$ is a solvable group.

*Proof.* Write $K = F(\alpha_1, \ldots, \alpha_r)$ with $\alpha_i^{n_i} \in F(\alpha_1, \ldots, \alpha_{i-1})$ and let $n = \text{lcm}\{n_i\}$. Then $K(\zeta_n)/F$ is also normal (if $K/F$ is the sf of $\mathcal{F}$ then $K(\zeta_n)/F$ is the sf of $\mathcal{F} \cup \{X^n - 1\}$). Also $K(\zeta_n) = F(\zeta_n, \alpha_1, \ldots, \alpha_r)$ and $F(\zeta_n, \alpha_1, \ldots, \alpha_r)$ is the sf of $X^n - \alpha_i^{n_i}$ over $F(\zeta_n, \alpha_1, \ldots, \alpha_{i-1})$. Hence if $H_i = \text{Gal}(K(\zeta_n)/F(\zeta_n, \alpha_1, \ldots, \alpha_i))$ then $H_i \leq H_{i-1}$ and $H_{i-1}/H_i$ is cyclic. Also $H_0 = \text{Gal}(K(\zeta_n)/F(\zeta_n)) \leq G = \text{Gal}(K(\zeta_n)/F)$ and $G/H_0 \leq (\mathbb{Z}/n\mathbb{Z})^\times$ is abelian. But $H_r = \{1\}$, so $G$ is solvable. Now $\text{Gal}(K/F)$ is a quotient of $G$, so is also solvable.

**Corollary** There exist quintics that do not have roots in any radical extension.

*Proof.* There exist quintics $f$ over $\mathbb{Q}$ with Galois group $S_5$. If $K/\mathbb{Q}$ were a radical extension containing a root of $f$ then its normal closure $M/\mathbb{Q}$ would be a radical extension containing all roots of $f$. But then $M$ would contain a sf $L$ for $f$ and $\text{Gal}(L/\mathbb{Q})$ would be a quotient group of $\text{Gal}(M/\mathbb{Q})$ which is solvable. Hence $\text{Gal}(L/\mathbb{Q}) \cong S_5$ would be solvable, a contradiction.

**Theorem 4** If $K/F$ is Galois with solvable Galois group then $K$ is contained in a radical extension of $F$.

*Proof.* Let $n = [K:F]$. Then $\text{Gal}(K(\zeta_n)/F)$ is solvable [$\text{Gal}(K(\zeta_n)/K)$ is an abelian normal subgroup with solvable quotient $\text{Gal}(K/F)$]. Hence $G = \text{Gal}(K(\zeta_n)/F(\zeta_n))$ is solvable [$\leq \text{Gal}(K(\zeta_n)/F)$]. The map $G \to \text{Gal}(K/F)$ obtained by restricting $g \in G$ to $K$ is an injective homomorphism [if $g$ fixes $K$ and $F(\zeta_n)$ then it clearly fixes $K(\zeta_n)$, so $|G| | n$. Thus there is a sequence $1 = H_0 \leq H_1 \leq \ldots \leq H_r = G$ with $H_i/H_{i-1}$ cyclic and if $L_i = K(\zeta_n)_{H_i}$ then $L_{i-1}/L_i$ is a Galois extension with cyclic Galois group of order $n_i | [H_i/H_{i-1}] | n$, so $\zeta_{n_i} \in L_i$. Thus $L_{i-1} = L_i(\alpha_i)$ for some $\alpha_i$ with $\alpha_i^{n_i} \in L_i$ and $L_r = F(\zeta_n)$. Thus $L_0 = K(\zeta_n)$ is radical over $F$ and contains $K$. 


Any finite Galois extension has a finite number of intermediate fields since these just correspond to subgroups of a finite group. The following lemma gives a criterion for when this happens in general.

**Lemma 1** Let $K/F$ be a finite extension. Then $K/F$ has finitely many intermediate fields $L$, $F \subseteq L \subseteq K$, if and only if $K/F$ is simple, i.e., $K = F(\alpha)$ for some $\alpha \in K$.

**Proof.** Assume first that $K = F(\alpha)$ is simple. Let $L$ be an intermediate field and consider $m_{\alpha,L}$. Now $m_{\alpha,L} \mid m_{\alpha,F}$ in $L[X]$ since $m_{\alpha,F}(\alpha) = 0$. Thus $m_{\alpha,L}$ is a factor of $m_{\alpha,F}$ in $K[X]$. But if $m_{\alpha,F} = f_1 f_2 \ldots f_r$ in $K[X]$ with $f_i$ irreducible, then by unique factorization in $K[X]$, $m_{\alpha,L}$ must be some product of some of the $f_i$. Hence there are at most $2^r$ possible values for $m_{\alpha,L}$. If $m_{\alpha,L} = \sum_{i=0}^m b_i X^i$, let $M = F(b_0, \ldots, b_m)$. Clearly $M \subseteq L$ so $m_{\alpha,L} \mid m_{\alpha,M}$ since $m_{\alpha,M} \in L[X]$ and $m_{\alpha,M}(\alpha) = 0$. However $m_{\alpha,L} \in M[X]$ so $m_{\alpha,M} \mid m_{\alpha,L}$. Thus $m_{\alpha,L} = m_{\alpha,M}$. Now $K = F(\alpha) \subseteq M(\alpha) \subseteq L(\alpha) \subseteq K$, and $[L(\alpha) : L] = [M(\alpha) : M] = \deg m_{\alpha,L}$, so $[K : L] = [K : M]$ and $M = L$. Since $m_{\alpha,L}$ determines $M = L$ and there are only finitely many possible $m_{\alpha,L}$s, there can be only finitely many $L$s.

Now assume there are only finitely many intermediate fields. We shall first consider the case when $F$ is infinite. Since $K/F$ is finite, $K = F(\alpha_1, \ldots, \alpha_r)$ for some $\alpha_i \in K$ (e.g., take the $\alpha_i$ to be a basis for $K/F$). We shall show that for any $\alpha, \beta \in K$, $F(\alpha, \beta) = F(\gamma)$ for some $\gamma \in K$. The result will then follow by taking $r$ above to be minimal and noting that $F(\alpha_1, \ldots, \alpha_r) = F(\alpha_1, \alpha_2)(\alpha_3, \ldots, \alpha_r) = F(\gamma, \alpha_3, \ldots, \alpha_r)$ for some $\gamma$.

Let $\gamma = \alpha + c \beta$ for some $c \in F$. Then $F(\gamma)$ is some intermediate field. Since there are only finitely many intermediate fields and $F$ is infinite, there exists $c_1, c_2 \in F$ with $F(\alpha + c_1 \beta) = F(\alpha + c_2 \beta)$. Call this field $L$. Then $(c_1 - c_2)\beta = (\alpha + c_1 \beta) - (\alpha + c_2 \beta) \in L$. Also $c_1 - c_2 \in F \subseteq L$, so $\beta \in L$. Now $\alpha = (\alpha + c_1 \beta) - c_1 (\beta) \in L$, so $F(\alpha, \beta) \subseteq L$. Clearly $L \subseteq F(\alpha, \beta)$, so $F(\alpha, \beta) = F(\alpha + c_1 \beta)$ as required.

If $F$ is finite then $|K| = |F|^{[K:F]} < \infty$, so $K$ is finite. Then $K^\times$ is cyclic, generated by $\alpha$ say, so $K = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^r\}$ and $K = F(\alpha)$.

**Theorem (The Theorem of the Primitive Element)** If $K/F$ is finite and separable then $K = F(\alpha)$ for some $\alpha \in K$.

**Proof.** Let $M$ be the normal closure of $K/F$, so $M/F$ is finite and Galois. By the fundamental theorem of Galois theory, there are only finitely many fields $L$ with $F \subseteq L \subseteq M$. Hence there are only finitely many fields with $F \subseteq L \subseteq K$. Hence $K/F$ is simple by Lemma 1.

**Example** Let $K = \mathbb{F}_p(x, y)$ where $x$, $y$ are indeterminants. Let $F = \mathbb{F}_p(x^p, y^p) \subseteq K$. Then $\{x^iy^j : 0 \leq i, j < p\}$ is a basis of $K/F$ so any $\gamma \in K$ is of the form $\sum a_{ij} x^i y^j$ with $a_{ij} \in F$. Now $\gamma^p = \sum a_{ij}^p x^{pi} y^{pj} \in F$, so $[F(\gamma) : F] \leq p$. But $[K : F] = p^2$, so $K/F$ is not simple and has an infinite number of intermediate fields.
Assume $K/F$ is a finite extension with $[K:F] = n$. Then $K$ can be regarded as an $n$-dimensional $F$-vector space. If $\alpha \in K$ then the map $t_\alpha : K \to K$ which sends $\beta$ to $\alpha\beta$ is an $F$-linear map from the $F$-vector space $K$ to itself, and as such can be represented by an $n \times n$ matrix with coefficients in $F$.

**Definition** The *norm* of an element $\alpha \in K$ is the determinant $N_{K/F}(\alpha) = \det t_\alpha$ and the *trace* of $\alpha$ is the trace $\text{Tr}_{K/F}(\alpha) = \text{tr} t_\alpha$ of the matrix representing $t_\alpha$. Note that both these quantities are independent of the basis for $K/F$.

**Theorem 1**

(a) $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$ and $\text{Tr}_{K/F}(\alpha + \beta) = \text{Tr}_{K/F}(\alpha) + \text{Tr}_{K/F}(\beta)$.

(b) If $K/L/F$ and $\alpha \in L$ then $N_{K/F}(\alpha) = N_{L/F}(\alpha)^{[K:L]}$ and $\text{Tr}_{K/F}(\alpha) = [K:L] \text{Tr}_{L/F}(\alpha)$.

(c) If $m_{\alpha,F} = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ then $N_{F/(\alpha)}(\alpha) = (-1)^n a_0$ and $\text{Tr}_{F/(\alpha)}(\alpha) = -a_{n-1}$.

(d) If $K/F$ is Galois, $N_{K/F}(\alpha) = \prod_{g \in \text{Gal}(K/F)} g(\alpha)$ and $\text{Tr}_{K/F}(\alpha) = \sum_{g \in \text{Gal}(K/F)} g(\alpha)$.

**Proof.**

(a) Follows from standard properties of det and tr using $t_{\alpha\beta} = t_\alpha \circ t_\beta$ and $t_{\alpha+\beta} = t_\alpha + t_\beta$.

(b) Let $\{\alpha_i\}$ be a basis for $L/F$ and $\{\beta_j\}$ be a basis for $K/L$. Then by the tower law $\{\alpha_i\beta_j\}$ is a basis for $K/F$. In this basis, $t_\alpha(K/F)$ is represented as a matrix with blocks corresponding to $t_\alpha(L/F)$ down the diagonal and zeros elsewhere. Thus $\det t_\alpha(K/F) = (\det t_\alpha(L/F))^r$ and $\text{tr} t_\alpha(K/F) = r \text{tr} t_\alpha(L/F)$ where $r = [K:L]$ is the number of blocks.

(c) Use a basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ for $F(\alpha)/F$. Then the matrix $t_\alpha$ will be of the form

\[
\begin{pmatrix}
0 & 0 & \ldots & 0 & -a_0 \\
1 & 0 & \ldots & 0 & -a_1 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \ldots & 1 & -a_{n-1}
\end{pmatrix}
\]

(d) $N_{K/F}(\alpha) = N_{F/(\alpha)}(\alpha)^r = (\pm a_0)^r = \prod \alpha_i^r$ where $r = [K:F(\alpha)]$, and $\alpha = \alpha_1, \alpha_2, \ldots$ are the roots of $m_{\alpha,F}$. Let $G = \text{Gal}(K/F)$ and let $H = \text{Gal}(K/F(\alpha))$. For each $i$ there exists a $g \in G$ with $g(\alpha) = \alpha_i$. Moreover if $g' \alpha = \alpha_i$ then $g^{-1}g' \alpha$ fixes $\alpha$, so $g^{-1}g' \in H$ and $g' \in gH$. Conversely if $g' \in gH$ then $g'(\alpha) = g(\alpha) = \alpha_i$. Hence

\[
\prod_{g \in G} g(\alpha) = \prod_{gH \in G/H} \prod_{g' \in gH} g'(\alpha) = \prod_{gH \in G/H} \alpha_i^{[H]} = \prod \alpha_i^{[H]} = N_{K/F}(\alpha).
\]

A similar argument works for Tr.

**Exercises**

1. Show that if $K/L/F$ and both $K/F$ and $L/F$ are Galois then $N_{K/F}(\alpha) = N_{L/F}N_{K/L}(\alpha)$ and $\text{Tr}_{K/F}(\alpha) = \text{Tr}_{L/F} \text{Tr}_{K/L}(\alpha)$. [In fact this is true for any finite $K/L/F$.]

2. Describe the functions $N_{\mathbb{C}/\mathbb{R}}$ and $\text{Tr}_{\mathbb{C}/\mathbb{R}}$ explicitly.