AGENDA

- FIELD AND FIELD EXTENSIONS
  - FIELD AXIOMS
  - ALGEBRAIC EXTENSIONS
  - TRANSCENDENTAL EXTENSIONS

- TRANSCENDENTAL EXTENSIONS
  - TRANSCENDENCE BASE
  - TRANSCENDENCE DEGREE

- NOETHER’S NORMALIZATION THEOREM
  - SKETCH OF PROOF
  - RELEVANCE
**Definition:** A field is a non-empty set $F$ with two binary operations on $F$, namely, “+” (addition) and “·” (multiplication), satisfying the following field axioms:

<table>
<thead>
<tr>
<th>Property</th>
<th>Addition</th>
<th>Multiplication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Closure</td>
<td>$x + y \in F$, for all $x, y \in F$</td>
<td>$x \cdot y \in F$, for all $x, y \in F$</td>
</tr>
<tr>
<td>Commutativity</td>
<td>$x + y = y + x$, for all $x, y \in F$</td>
<td>$x \cdot y = y \cdot x$, for all $x, y \in F$</td>
</tr>
<tr>
<td>Associativity</td>
<td>$(x + y) + z = x + (y + z)$, for all $x, y, z \in F$</td>
<td>$(x \cdot y) \cdot z = x \cdot (y \cdot z)$, for all $x, y, z \in F$</td>
</tr>
<tr>
<td>Identity</td>
<td>There exists an element $0 \in F$ such that $0 + x = x$ and $0 = x$, for all $x \in F$ (Additive Identity)</td>
<td>There exists an element $1 \in F$ such that $1 \cdot x = x \cdot 1 = x$, for all $x \in F$ (Multiplicative Identity)</td>
</tr>
<tr>
<td>Inverse</td>
<td>For all $x \in F$, there exists $y \in F$ such that $x + y = 0$ (Additive Inverse)</td>
<td>For all $x \in F^\times$, there exists $y \in F$ such that $x \cdot y = 1$ (Multiplicative Inverse)</td>
</tr>
<tr>
<td>Distributivity (Multiplication is distributive over addition)</td>
<td>For all $x, y, z \in F$, $x \cdot (y + z) = x \cdot y + x \cdot z$</td>
<td></td>
</tr>
</tbody>
</table>
EXAMPLES

• Set of Real Numbers, \( \mathbb{R} \)
• Set of Complex Numbers, \( \mathbb{C} \)
• Set of Rational Numbers, \( \mathbb{Q} \)
• \( \mathbb{F}_2 = \{0,1\} = \mathbb{Z}/2\mathbb{Z} \)
• In general, \( \mathbb{F}_p = \{0,1, \ldots, p - 1\} = \mathbb{Z}/p\mathbb{Z} \), where \( p \) is prime
• \( \mathbb{C}(X) \), the field of rational functions with complex coefficients
• \( \mathbb{R}(X) \), the field of rational functions with real coefficients
• \( \mathbb{Q}(X) \), the field of rational functions with rational coefficients
• In general, \( K(X) \), where \( K \) is a field
EXTENSION FIELDS

**Definition:** A field $E$ containing a field $F$ is called an extension field of $F$ (or simply an extension of $F$, denoted by $E/F$). Such an $E$ is regarded as an $F$–vector space. The dimension of as an $F$–vector space is called the degree of $E$ over $F$ and is denoted by $[E:F]$. We say $E$ is finite over $F$ (or a finite extension of $F$) if it has a finite degree over $F$ and infinite otherwise.

**Examples:**

(a) The field of complex numbers, $\mathbb{C}$, is a finite extension of $\mathbb{R}$ and has degree 2 over $\mathbb{R}$ (basis $\{1, i\}$)

(b) The field of real numbers, $\mathbb{R}$, has an infinite degree over the field of rationals, $\mathbb{Q}$: the field $\mathbb{Q}$ is countable, and so every finite-dimensional $\mathbb{Q}$–vector space is also countable, but a famous argument of Cantor shows that $\mathbb{R}$ is not countable.

(c) The field of Gaussian rationals, $\mathbb{Q}(i) = \{a + bi: a, b \in \mathbb{Q}\}$, has degree 2 over $\mathbb{Q}$ (basis $\{1, i\}$)

(d) The field $F(X)$ has infinite degree over $F$; in fact, even its subspace $F[X]$ has infinite dimension over $F$.
**ALGEBRAIC AND TRANSCENDENTAL ELEMENTS**

**Definition:** An element $\alpha$ in $E$ is *algebraic* over $F$, if $f(\alpha) = 0$, for some non-zero polynomial $f \in F[X]$. An element that is not algebraic over $F$ is *transcendental* over $F$.

**Examples:** (a) The number $\alpha = \sqrt{2}$ is algebraic over $\mathbb{R}$ since $p(\sqrt{2}) = 0$, for $p(X) = X^2 - 2 \in \mathbb{R}[X]$
(b) The number $\alpha = \sqrt[3]{3}$ is algebraic over $\mathbb{Q}$ since $h(\sqrt[3]{3}) = 0$, for $h(X) = X^3 - 3 \in \mathbb{Q}[X]$
(c) The number $\pi = 3.141 \ldots$ is transcendental over $\mathbb{Q}$
(d) The number $\alpha = \pi$ is algebraic over $\mathbb{Q}(\pi)$ since $q(\pi) = 0$ for $q(X) = X - \pi \in \mathbb{Q}(\pi)[X]$
**Definition:** A field extension $E/F$ is said to be an *algebraic extension*, and $E$ is said to be algebraic over $F$, if all elements of $E$ are algebraic over $F$. Otherwise, $E$ is transcendental over $F$. Thus, $E/F$ is *transcendental* if at least one element of $E$ is transcendental over $F$.

**Remark:** A field extension $E/F$ is finite if and only if $E$ is algebraic and finitely generated (as a field) over $F$.

**Examples:**
(a) The field of real numbers is a transcendental extension of the field $\mathbb{Q}$ since $\pi$ is transcendental over $\mathbb{Q}$
(b) The field $\mathbb{Q}(e)$ is a transcendental extension of $\mathbb{Q}$ since $e$ is transcendental over $\mathbb{Q}$
(c) The field of rational functions $F(X)$ in the variable $X$ is a transcendental extension of the field $F$ since $X$ is transcendental over $F$.
(d) The field $\mathbb{Q}(\sqrt{2})$ is an algebraic extension of $\mathbb{Q}$ since it has degree 2 (finite) over $\mathbb{Q}$
(e) The field $\mathbb{Q}(\sqrt[3]{3})$ is an algebraic extension of $\mathbb{Q}$ since it has degree 3 (finite) over $\mathbb{Q}$
Definition: A subset $S = \{a_1, ..., a_n\}$ of $E$ is called *algebraically independent* over $F$ if there is no non-zero polynomial $f(x_1, ..., x_n) \in F[X_1, ..., X_n]$ such that $f(a_1, ..., a_n) = 0$. A *transcendence base* for $E/F$ is a maximal subset (with respect to inclusion) of $E$ which is algebraically independent over $F$.

Note that if $E/F$ is an algebraic extension, the empty set is the only algebraically independent subset of $E$. In particular, elements of an algebraically independent set are necessarily transcendental.
**Theorem:** The extension $E/F$ has a transcendence base and any two transcendence bases of $E/F$ have the same cardinality.

**Remark:** The *cardinality of a transcendence base* for $E/F$ is called the *transcendence degree* of $E/F$. Algebraic extensions are precisely the extensions of transcendence degree 0. Note that if $S_1$ and $S_2$ are transcendence bases for $E/F$, it is not necessarily the case that $F(S_1) = F(S_2)$. 
**Theorem:** Suppose that $R$ is a finitely generated domain over a field $K$. Then, there exists an algebraically independent subset $\mathcal{L} = \{y_1, \ldots, y_r\}$ of $R$ so that $R$ is integral over $R[\mathcal{L}]$

**Sketch Of The Proof:**

**Definition:** In commutative algebra, an element $b$ of a commutative ring $B$ is said to be integral over $A$, a subring of $B$, if $b$ is a root of a monic polynomial over $A$. If every element of $B$ is integral over $A$, then $B$ is said to be integral over $A$.

(i) The proof is done by induction on $n$, the number of generators of $R$ over $K$. Thus, $R = K[x_1, \ldots, x_n]$

(ii) If $n = 0$, then $R = K$ (Nothing to Prove). If $n = 1$, then $R = K[x_1]$. Then, there are two cases:

(a) If $x_1$ is algebraic, then $r = 0$ and $x_1$ is integral over $K$. So, the theorem holds.

(b) If $x_1$ is transcendental, then set $x_1 = y_1$. Then, we get $R = K[x_1]$, which is integral over $K[x_1]$. 

(iii) Now, let $n \geq 2$. If $x_1, \ldots, x_n$ are algebraically independent, then set $x_i = y_i, \forall i$ and we’re done. If not, then there exists a non-zero polynomial $f(X) \in K[X_1, \ldots, X_n]$ such that $f(x_1, \ldots, x_n) = 0.$
The polynomial can be written as $f(X) = \sum_\alpha c_\alpha X^\alpha$, where we use the notation $X^\alpha = X_1^{a_1} \cdots X_n^{a_n}$ for $\alpha = (a_1, \ldots, a_n)$.

(iv) Rewriting the above polynomial as a polynomial in $X_1$ with coefficients in $K[X_2, \ldots, X_n]$, we have:

$$f(X) = \sum_{j=0}^N f_j(X_1, \ldots, X_n)X_1^j$$

Since $f$ is non-zero, it involves at least one of the $X_i$ and we can assume it is $X_1$. Now, we want to somehow arrange to have $f_N = 1$. Then, $x_1$ would be integral over $K[x_2, \ldots, x_n]$, which by induction on $n$ would be integral over $K[\mathcal{L}]$, for some algebraically independent subset $\mathcal{L}$. Since the integral extensions of integral extensions are integral, the theorem follows.

(v) To make $f$ monic, we perform a change of variables that transforms or “normalizes” $f$ into a monic polynomial in $X_1$. Let $Y_2, \ldots, Y_n$ and $y_2, \ldots, y_n \in R$ be given by $Y_i = X_i - X_1^{m_i}$, where the positive integers $m_i = d^{i-1}$, where $d$ is an integer greater than any of the exponents which occur in the polynomial $f(X)$. This gives us a new polynomial $g(X_1, Y_2, \ldots, Y_n) = f(X_1, \ldots, X_n) \in K[X_1, Y_2, \ldots, Y_n]$ such that $g(x_1, y_2, \ldots, y_n) = 0$. Then,

$$g(X_1, Y_2, \ldots, Y_n) = \sum_\alpha c_\alpha X_1^{a_1} (X_1^d + X_2)^{a_2} (X_1^{d^2} + X_3)^{a_3} \cdots (X_1^{d^{n-1}} + X_n)^{a_n}$$
It is easy to see that $K[X_1, Y_2, \ldots, Y_n] = K[X_1, X_2, \ldots, X_n]$. Now, the highest power of $X_1$ which occurs is $N = \sum a_i d^{i-1}$. The coefficient of $X_1^N$ is $c_\alpha$. We can divide $g$ by this non-zero constant and make $g$ monic in $X_1$ and we’re done by induction.

**Relevance:** Noether’s Normalization Theorem provides a refinement of the choice of transcendental extensions so that certain ring extensions are integral extensions, not just algebraic extensions.
REFERENCES

• Algebra, Serge Lange (Revised Third Edition)
• Abstract Algebra, David S. Dummit & Richard M. Foote
• Abstract Algebra Theory And Applications, Thomas W. Judson
• Fields And Galois Theory, J. S. Milne
• Galois Theory, Ian Stewart