IV. Algebraic Extensions & Algebraic Closures

**Definition 1.** Let $E$ be a field and let $F$ be a subset of $E$. Then $F$ is a subfield of $E$ if $F$ is also a field under the operations of $E$.

If $E$ is a field containing the subfield $F$, then $E$ is said to be an extension field (or just extension) of $F$, denoted $E/F$ (read “$E$ over $F$”).

**Definition 2.** Let $F$ be a field and $E$ be an extension of $F$.

1. An element $a \in E$ is said to be algebraic over $F$ if $a$ is a root of some nonzero polynomial $f(x) \in F[x]$.

2. If $a$ is not algebraic over $F$ (i.e., $a$ is not the root of any nonzero polynomial with coefficients in $F$) then $a$ is said to be transcendental over $F$.

3. The extension $E/F$ is said to be algebraic if every element of $E$ is algebraic over $F$.

**Example 3.**

1. Every element $a$ of a field $F$ is algebraic over $F$. Moreover, if $E/F$ is an extension field and $a \in E$ is algebraic over $F$, then $a$ is algebraic over any extension field $K$ of $F$.

2. $\mathbb{C}/\mathbb{R}$ is an algebraic extension.

3. There are real numbers that are transcendental over $\mathbb{Q}$.

4. The complex number $2\pi i$ is algebraic over $\mathbb{R}$, but transcendental over $\mathbb{Q}$.

**Definition 4.** Let $E$ be an extension of the field $F$ and let $a, b, \ldots \in E$ be a collection of elements of $E$. Then the smallest subfield of $E$ containing both $F$ and the elements $a, b, \ldots$, denoted $F(a, b, \ldots)$, is called the field generated by $a, b, \ldots$ over $F$.

If the field $E$ is generated by a single element $a$ over $F$, $E = F(a)$, then $E$ is said to be a simple extension of $F$ and the element $a$ is called a primitive element for the extension.

**Theorem 5.** Let $E$ be an extension of the field $F$, $a \in E$ and let $F(a)$ be the field generated by $a$ over $F$.

1. If $a$ is transcendental over $F$, then $F(a) \cong F(x)$.

2. If $a$ is a root of an irreducible polynomial $p(x) \in F[x]$, then $F(a) \cong F[x]/(p(x))$.

If $\deg(p(x)) = n$, then every element of $F(a)$ can be uniquely expressed in the form

$$c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1a + c_0,$$

where $c_0, c_1, \ldots, c_{n-1} \in F$. 
Example 6. Describe the elements of the field \( \mathbb{Q}(\sqrt{2}) \).

Note: If \( E/F \) is an extension of fields, then the multiplication defined on \( E \) makes \( E \) into a vector space over \( F \).

Definition 7. The degree of a field extension \( E/F \), denoted \( [E:F] \), is the dimension of \( E \) as a vector space over \( F \) (i.e., \( [E:F] = \dim_F E \)). The extension is said to be finite if \( [E:F] \) is finite and otherwise is said to be infinite.

The last part of Theorem 5 (2) can be restated in the language of vector spaces:

Theorem 8. Let \( a \) be a root of an irreducible polynomial of degree \( n \) over a field \( F \). Then the set \( \{1, a, \ldots, a^{n-1}\} \) is a basis for \( F(a) \) as a vector space over \( F \), and \( [F(a):F] = n \).

Example 9. Find the following degrees.

1. \( [\mathbb{C}:\mathbb{R}] \)
2. \( [\mathbb{R}:\mathbb{Q}] \)

Corollary 10. Let \( F \) be a field and let \( p(x) \in F[x] \) be irreducible over \( F \). If \( a, b \) are roots of \( p(x) \) in some extensions \( E \) and \( E' \) of \( F \), respectively, then \( F(a) \cong F(b) \).

Example 11.

1. \( \mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(-\sqrt{2}) \).
2. \( \mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}\left(\sqrt{2}\left(\frac{-1+i\sqrt{3}}{2}\right)\right) \cong \mathbb{Q}\left(\sqrt{2}\left(\frac{-1-i\sqrt{3}}{2}\right)\right) \).
Theorem 12. Let $E/F$ be an extension of a field $F$ and let $a$ be algebraic over $F$. Then there is a unique monic irreducible polynomial $m_{a,F}(x) \in F[x]$ which has $a$ as a root. A polynomial $f(x) \in F[x]$ has $a$ as a root if and only if $m_{a,F}(x)$ divides $f(x)$ in $F[x]$.

Corollary 13. If $E/F$ is an extension of fields and $a$ is algebraic over both $F$ and $E$, then $m_{a,E}(x)$ divides $m_{a,F}(x)$ in $E[x]$.

Definition 14. The polynomial $m_{a,F}(x)$ in Theorem 12 is called the minimal polynomial for $a$ over $F$. The degree of $m_{a,F}(x)$ is called the degree of $a$.

Note: By Theorem 12, a monic polynomial over $F$ with $a$ as a root is the minimal polynomial for $a$ over $F$ if and only if it is irreducible over $F$.

Theorem 15. Let $a$ be algebraic over the field $F$ and let $F(a)$ be the field generated by $a$ over $F$. Then $F(a) \cong F[x]/(m_{a,F}(x))$.

In particular, $[F(a) : F] = \deg (m_{a,F}(x)) = \deg a$.

Example 16. Let $n \in \mathbb{Z}^+$. Find the following degrees

1. $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}]$

2. $[\mathbb{R}(\sqrt[n]{2}) : \mathbb{R}]$

3. $[\mathbb{Q}(a) : \mathbb{Q}]$, where $a$ is any root of $p(x) = x^4 + 10x + 5$

Theorem 17. If the extension $E/F$ is finite, then $E$ is algebraic over $F$.

Note: The converse of Theorem 17 is not true as the following example shows.

Example 18. $\mathbb{Q}(\sqrt{2}, \sqrt{2}, \sqrt{2}, \ldots)$ is an algebraic extension of $\mathbb{Q}$ but not a finite extension of $\mathbb{Q}$.

Theorem 19. Let $F \subseteq L \subseteq E$ be fields. Then $[E : F] = [E : L][L : F]$.

If one side of the above equation is infinite, then the other side is also infinite.

Example 20.

1. Find the following degrees.

   (a) $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}(\sqrt{2})]$

   (b) $[\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}]$

2. Note that $\sqrt{2} \notin \mathbb{Q}(a)$, where $a$ is any root of $p(x) = x^4 + 10x + 5$. 
Definition 21. A field $F$ is algebraically closed if every nonconstant polynomial with coefficients in $F$ has root in $F$ (equivalently all roots are in $F$).

The extension field $\overline{F}$ of $F$ is called an algebraic closure of $F$ if $\overline{F}$ is algebraic over $F$ and every nonconstant polynomial in $F[x]$ has a root in $\overline{F}$.

Note: By the definition, $\overline{F}$ contains all the elements that are algebraic over $F$.

Lemma 22. Let $F \subset L \subset E$ be a tower of fields. If $E/L$ is an algebraic extension and $L/F$ is an algebraic extension, then $E/F$ is an algebraic extension.

Proposition 23. Let $\overline{F}$ be an algebraic closure of $F$. Then $\overline{F}$ is algebraically closed.

Proposition 24. For any field $F$ there exists a unique (up to isomorphism) algebraic closure of $F$.

Example 25.

1. (Fundamental Theorem of Algebra) The field $\mathbb{C}$ is algebraically closed.

2. The field $\mathbb{C}$ contains an algebraic closure for any of its subfields. In particular, $\overline{\mathbb{Q}}$, the collection of complex numbers algebraic over $\mathbb{Q}$, is the algebraic closure of $\mathbb{Q}$ and is contained properly in $\mathbb{C}$.

3. If $E$ is a finite extension of $\mathbb{R}$, then either $E = \mathbb{R}$ or $E = \mathbb{C}$.
Homework IV:

1. (a) (Subfield test) Let $E$ be a field and let $F$ be a subset of $E$ with at least two elements. Prove that $F$ is a subfield of $E$ if, for any $a, b \in F$ ($b \neq 0$), $a - b$ and $ab^{-1}$ belong to $F$.

(b) $\star$ Let $E$ be a field and $\{F_\alpha\}$ be a family of subfields of $E$. Prove that $\bigcap F_\alpha$ is a subfield of $E$.

2. $\star$ Let $F$ be a field and let $p(x) \in F[x]$. Prove the following: If $f(x), g(x) \in F[x]$ such that $\deg(f(x)) < \deg(p(x)), \deg(g(x)) < \deg(p(x))$, and $f(x)+(p(x)) = g(x)+(p(x))$ in $F[x]/(p(x))$, then $f(x) = g(x)$.

3. $\star$ (Eisenstein’s Criterion for $\mathbb{Z}[x]$) Let

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x], \ n \geq 1.$$ 

If there is a prime $p$ such that

(a) $p$ doesn’t divide $a_n$,

(b) $p$ divides $a_i$ for $i \in \{0, 1, \ldots, n - 1\}$, and

(c) $p^2$ doesn’t divide $a_0$,

then $f(x)$ is irreducible over $\mathbb{Q}$.

4. (a) Let $F$ be a field and let $p(x) \in F[x]$. Prove that $(p(x))$ is a maximal ideal in $F[x]$ if and only if $p(x)$ is irreducible in $F[x]$.

(b) Let $F$ be a field, $I$ a nonzero ideal in $F[x]$, and $g(x)$ an element of $F[x]$. Prove that $I = (g(x))$ if and only if $g(x)$ is a nonzero polynomial of minimal degree in $I$.

5. Let $D$ be an integral domain that contains a field $F$ as a subring. If $D$ is finite-dimensional when viewed as a vector space over $F$, prove that $D$ is a field.

6. $\star$ Let $F \subseteq L \subseteq E$ be fields. Prove that

$$[E : F] = [E : L][L : F].$$

If one side of the above equation is infinite, then the other side is also infinite.

7. $\star$ Let $E$ be an extension of a field $F$. Prove that $F(a, b) = [F(a)](b) = [F(b)](a)$.

8. (a) Prove that the polynomial $f(x) = x^4 + 2x^3 + 6x^2 + x + 9 \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x]$. (Hint: Use Mod $p$ Irreducibility Test (Homework II #8).)

(b) Let $a$ be a root of $f(x)$ in some extension of $\mathbb{Q}$. Prove that $\sqrt{2} \notin \mathbb{Q}(a)$.

9. $\star$ Let $F \subset L \subset E$ be fields. Prove that if $E/L$ is an algebraic extension, and $L/F$ is an algebraic extension, then $E/F$ is an algebraic extension.
10. Prove the following: The field $E$ is an algebraic closure of itself if and only if $E$ is algebraically closed.

11. Suppose that $F$ is a field and every irreducible polynomial in $F[x]$ is linear. Prove that $F$ is algebraically closed.