If \( F \) is a field which is a subset of a bigger field, \( K \), then \( K \) is called an extension. It is written \( K/F \).

**Definition.** Given a field extension \( K/F \), the degree of the extension, \([K : F]\) is the dimension of \( K \) as a vector space over \( F \).

The element, 1, is in every field, we may consider
\[
\frac{1 + 1 + \ldots + 1}{n \text{ times}} = n.1
\]
then for each \( n \), we either obtain a new element, or 0.

**Definition.** The characteristic of a field, \( F \), is the smallest number, \( p \), such that \( p.1 = 0 \) and 0 if none exists. It is denoted \( \text{char}(F) \). If \( \text{char}F \neq 0 \), then it is prime.

**Definition.** The field generated by identity element is called the prime (or base) field, and it is isomorphic to either \( \mathbb{Q} \) or \( \mathbb{Z}_p \) for some prime.

Given a field, \( F \), and an irreducible polynomial, \( p(x) \), we can form the field extension \( \mathbb{K} = \mathbb{F}[x]/\langle p(x) \rangle \), which contains a solution of \( p(x) \). If \( p(x) \) is irreducible, then \( \langle p(x) \rangle \) is maximal, hence, \( K \) is a field.

**Theorem 13.4.** The degree of the extension is \([K : F] = \deg p(x)\). If \( \varphi : \mathbb{F}[x] \to \mathbb{K} \) and \( \varphi(x) = \theta \), then \( \{1, \theta, \ldots, \theta^n\} \) is a basis for \( K \) over \( F \).

We call \( \alpha \in K \) algebraic over \( F \) if there exists a polynomial \( p(x) \in \mathbb{F}[x] \) such that \( p(\alpha) = 0 \) in \( K \).

**Definition.** Given an algebraic element, \( \alpha \in K \), over \( F \) the irreducible monic polynomial with \( \alpha \) as a solution is called the minimal polynomial, \( m_\alpha(x) \).

**Corollary 13.10.** If \( \alpha \in K \) is algebraic and \( f(x) \in \mathbb{F}(x) \), \( f(\alpha) = 0 \) if and only if \( m_\alpha(x) | f(x) \).

A field extension is called algebraic if all its elements are algebraic.

**Definition.** The field \( \mathbb{F}(\alpha_1, \ldots, \alpha_n) \) is the smallest field containing \( \mathbb{F} \) and \( \alpha_1, \ldots, \alpha_n \). A field \( K \) is called a finite extension if \( K = \mathbb{F}(\alpha_1, \ldots, \alpha_n) \) and is called simple if \( n = 1 \).

**Proposition 13.11.** If \( \alpha \) is algebraic, then
\[
\mathbb{F}(\alpha) = \mathbb{F}[x]/\langle m_\alpha(x) \rangle, \quad [\mathbb{F}(\alpha) : \mathbb{F}] = \deg m_\alpha(x).
\]

**Theorem 13.14.** If \( F \subseteq K \subseteq L \), then
\[
[L : F] = [L : K][K : F].
\]
Hence, \([K : F] \) divides \([L : F] \) for any subfield \( K \).

**Definition.** Given two fields, \( K_1 \) and \( K_2 \), the composite field, \( K_1K_2 \) is the smallest field containing both \( K_1 \) and \( K_2 \).

**Definition.** An extension \( K/F \) is called a splitting field for \( f(x) \in F[x] \) if \( f(x) \) splits into linear factors over \( K \) and no proper subfield of \( K \).

**Important example**
\[
f(x) = x^n - 1.
\]
The splitting field is the cyclotomic extension \( \mathbb{Q}(\zeta_n) \), where \( \zeta_n = \exp(2\pi i/n) \). The degree is
\[
[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)
\]
where \( \varphi \) is Euler totient function.

**Definition.** A polynomial is called separable if it has no multiple roots.

**Proposition 13.33.** A polynomial \( f(x) \) is separable if and only if
\[
(D_x f(x), f(x)) = 1
\]
where \( D_x = d/dx \).

Another important example is \( f(x) = x^p - x \) over \( \mathbb{F}_p \). \( D_x f(x) = -1 \), hence, it is separable. If \( \alpha, \beta \) are roots, then so is \( \alpha + \beta \) and \( \alpha \beta \), \( \alpha^{-1} \) and \( \beta^{-1} \). There are \( p^n \) distinct roots, forming the field \( \mathbb{F}_{p^n} \), where
\[
[\mathbb{F}_{p^n} : \mathbb{F}_p] = n.
\]
If \( K \) is characteristic \( p \), we define the Frobenius endomorphism
\[
\varphi_p : x \rightarrow x^p.
\]
**Definition.** A field, \( F \), of characteristic \( p \) is called perfect if \( \varphi_p(F) = F \).

The finite fields of the type \( \mathbb{F}_{p^n} \) are perfect. The multiplicative group, \( \mathbb{F}_{p^n}^\times \), is cyclic.

**Proposition 13.37.** Every irreducible over fields of characteristic \( 0 \) and perfect fields are separable.

The \( \zeta_n \) satisfy the cyclotomic polynomials, \( \Phi_n \), which are irreducible monic polynomials of degree \( \varphi(n) \). Furthermore
\[
x^n - 1 = \prod_{d|n} \Phi_d
\]
For example, \( \Phi_{15}(x) \) is determined by
\[
x^{15} - 1 = \Phi_{15}(x)\Phi_5(x)\Phi_3(x)\Phi_1(x)
\]
\[
= \Phi_{15}(x)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x - 1).
\]
which implies \( \Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 \).

**Definition.** For any field extension \( K/F \), we define the groups
- \( \text{Aut}(K) \) is the group of automorphisms of \( K \).
- \( \text{Aut}(K/F) \) is the subgroup of automorphisms of \( K \) fixing \( F \).

**Definition.** Given a subgroup of \( H \subseteq \text{Aut}(K) \), we call the field that is fixed by \( H \) the fixed field of \( H \).

**Definition.** A character, \( \chi \), of a group, \( G \), with values in a field, \( \mathbb{L} \), is a map
\[
\chi : G \rightarrow \mathbb{L}^\times.
\]
such that \( \chi(gh) = \chi(g)\chi(h) \).

A character is “almost” an embedding of fields when \( G \) is taken to be the multiplicative group of a field.

**Proposition 14.2.** If \( \alpha \in K \) is a root of some \( f(x) \in \mathbb{F}[x] \), then so is \( \sigma(\alpha) \) for any \( \sigma \in \text{Aut}(K) \).
DEFINITION. Let $\mathbb{K}/\mathbb{F}$ be a finite field extension. $\mathbb{K}$ is said to be Galois if $[\text{Aut}(\mathbb{K}/\mathbb{F})] = [\mathbb{K} : \mathbb{F}]$. In this case, we write $\text{Gal}(\mathbb{K}/\mathbb{F}) = \text{Aut}(\mathbb{K}/\mathbb{F})$.

THEOREM. Given an extension, $\mathbb{K}/\mathbb{F}$, the following are equivalent:
1. The field is Galois, $[\mathbb{K} : \mathbb{F}] = [\text{Aut}(\mathbb{K}/\mathbb{F})]$.
2. $\mathbb{K}$ is the splitting of a separable polynomial over $\mathbb{F}$.
3. $\mathbb{F}$ is the fixed field of $\text{Aut}(\mathbb{K}/\mathbb{F})$.
4. $\mathbb{K}$ is a finite, normal and separable extension of $\mathbb{F}$.

Let $\mathbb{K}/\mathbb{F}$ be Galois, with $G = \text{Gal}(\mathbb{K}/\mathbb{F})$, then there is a bijection

\[
\begin{array}{ccc}
\text{Subfields, E,} & \text{Subgroups,} \\
of \mathbb{K}, & H \text{ of } G, \\
containing \mathbb{F}. & \end{array}
\]

given by

\[
E \left\{ \begin{array}{c}
\text{Subgroup of} \\
of \text{elements of}
\end{array} \right\}
\leftrightarrow H
\]

and

\[
\left\{ \begin{array}{c}
The \text{fixed} \\
of \text{field of } H.
\end{array} \right\}
\]

which are inverses to each other. Furthermore
1. The correspondence is inclusion reversing, i.e., if $H_1$, $H_2$ correspond to $E_1$, $E_2$, and $E_1 \subset E_2$, then $H_2 \leq H_1$.
2. $[\mathbb{K} : \mathbb{F}] = [H]$ and $[\mathbb{E} : \mathbb{F}] = [G : H]$.
3. $\mathbb{K}/\mathbb{E}$ is Galois and $\text{Gal}(\mathbb{K}/\mathbb{E}) = \text{Gal}(\mathbb{K}/\mathbb{F})$.
4. $\mathbb{E}$ is Galois over $\mathbb{F}$ if and only if $H$ is normal in $G$. More generally, if $H$ not normal, then the isomorphisms of $\mathbb{E}$ are in one to one correspondence with the cosets, $\sigma H$, in $G$.
5. If $H_1$, $H_2$ correspond to $E_1$, $E_2$ then $E_1E_2$ corresponds to $H_1 \cap H_2$ and $E_1 \cap E_2$ corresponds to $H_1 \cap H_2$.

An important example is the finite group $\mathbb{F}_{p^n}/\mathbb{F}_p$,

\[
\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \varphi_p \rangle \cong \mathbb{Z}/n\mathbb{Z}.
\]

where $\varphi_p$ is the Frobenius endomorphism above.

PROPOSITION 14.15. Every finite group is isomorphic to some $\mathbb{F}_{p^n}$. The subfields of $\mathbb{F}_{p^n}$ are in one to one correspondence with the divisors of $n$.

THEOREM 14.15 (Primitive element theorem). If $\mathbb{K}/\mathbb{F}$ is finite and separable, then $\mathbb{K}/\mathbb{F}$ is simple.

In particular, the finite fields are simple. Each $\mathbb{F}_{p^n}$ arises in the form

\[
\mathbb{F}_{p^n}/\mathbb{F}_p = \langle p(x) \rangle
\]

for some irreducible $p(x)$. Moreover,

\[
x^{p^n} - x = \prod_{\text{pinned}} p(x)
\]

which means that the collection of $x^{p^n} - x$ contains all simple extensions.

COROLLARY 14.20. Suppose $\mathbb{K}_1/\mathbb{F}$ is Galois and $\mathbb{K}_2/\mathbb{F}$ is any extension, $(\mathbb{K}_1, \mathbb{K}_2 \subset \mathbb{L})$, then

\[
[\mathbb{K}_1\mathbb{K}_2 : \mathbb{F}] = [\mathbb{K}_1 : \mathbb{F}][\mathbb{K}_2 : \mathbb{F}]/[\mathbb{K}_1 \cap \mathbb{K}_2 : \mathbb{F}]
\]

COROLLARY 14.22. If $\mathbb{K}_1$ and $\mathbb{K}_2$ are Galois over $\mathbb{F}$, with $\mathbb{K}_1 \cap \mathbb{K}_2 = \mathbb{F}$, then

\[
\text{Gal}(\mathbb{K}_1\mathbb{K}_2/\mathbb{F}) \cong \text{Gal}(\mathbb{K}_1/\mathbb{F}) \times \text{Gal}(\mathbb{K}_2/\mathbb{F}).
\]

Conversely, given a Galois extension, $\mathbb{K}/\mathbb{F}$, if there exists a decomposition $\text{Gal}(\mathbb{K}/\mathbb{F}) \cong G_1 \times G_2$, then there exist subfields $\mathbb{K}_1$ and $\mathbb{K}_2$ such that $\mathbb{K}_1 \cap \mathbb{K}_2 = \mathbb{F}$ and $\mathbb{K} = \mathbb{K}_1\mathbb{K}_2$.

We have from this the Galois group for cyclotomic extensions. Let

\[
n = p_1^{a_1} \cdots p_k^{a_k}
\]

then

\[
\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \text{Gal}(\mathbb{Q}(\zeta_{p_1}^{a_1})/\mathbb{Q}) \times \cdots \times \text{Gal}(\mathbb{Q}(\zeta_{p_k}^{a_k})/\mathbb{Q})
\]

\[= (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^\times
\]

Conversely, any abelian group arises as a subgroup of some cyclotomic extension.

THEOREM. Let $\mathbb{F}$ not have characteristic 2, and $f(x)$ be a separable irreducible quadratic, given by

\[
f(x) = x^2 + ax + b
\]

then the discriminant is

\[
D = a^2 - 4b.
\]

If the splitting field of $f$, $\mathbb{K}/\mathbb{F}$, has Galois group

\[
\text{Gal}(\mathbb{K}/\mathbb{F}) = \left\{ \begin{array}{c}
\mathbb{Z}/2\mathbb{Z} \quad \text{if } D \text{ is not a square in } \mathbb{F}.
\text{1} \quad \text{if } D \text{ is a square in } \mathbb{F}.
\end{array} \right.
\]

THEOREM. Let $\mathbb{F}$ not have characteristic 2, and $f(x)$ be a separable irreducible cubic, given by

\[
f(x) = x^3 + ax^2 + bx + c,
\]

then its discriminant is

\[
D = a^2b^2 - 4b^3 - 4a^2c^2 - 27c^2 + 18abc.
\]

If the splitting field of $f$, $\mathbb{K}/\mathbb{F}$, has Galois group

\[
\text{Gal}(\mathbb{K}/\mathbb{F}) = \left\{ \begin{array}{c}
S_3 \quad \text{if } D \text{ is not a square in } \mathbb{F}.
A_3 = \mathbb{Z}/3\mathbb{Z} \quad \text{if } D \text{ is a square in } \mathbb{F}.
\end{array} \right.
\]

THEOREM. Let $\mathbb{F}$ not have characteristic 2, and $f(x)$ be a separable irreducible quartic, given by

\[
f(x) = x^4 + ax^3 + bx^2 + cx + d,
\]

then its resolvent cubic is

\[
r(x) = x^3 - bx^2 + (ac - 4d)x - (a^2d + c^2 - 4bd)
\]

and its discriminant is

\[
D = 18a^3bcd - 27a^4d^2 - 4a^2c^3 - 4a^2b^2d + a^2b^2c^2 + 144a^2b^3
\]

\[
d^2 - 6a^2c^2d - 80a^2b^2c + 18abc^3 - 192acd^2 + 16b^4d - 4b^3
\]

\[
c^2 - 12bd^2 + 14bc^2d - 27b^2 + 256b^3
\]

If $r(x)$ is irreducible the splitting field of $f$, $\mathbb{K}/\mathbb{F}$, has Galois group

\[
\text{Gal}(\mathbb{K}/\mathbb{F}) = \left\{ \begin{array}{c}
S_4 \quad \text{if } D \text{ is not a square in } \mathbb{F},
A_4 \quad \text{if } D \text{ is a square in } \mathbb{F},
\end{array} \right.
\]

otherwise, if $r(x)$ is reducible

\[
\text{Gal}(\mathbb{K}/\mathbb{F}) = \left\{ \begin{array}{c}
D_8 \text{ or } \mathbb{Z}/4\mathbb{Z}
\end{array} \right.
\]

If the root of $r(x)$ is $\alpha$, it is $\mathbb{Z}/4\mathbb{Z}$ if $x^2 - aX + b - \alpha$ and $x^2 - bX - \alpha + d$ both split over $\mathbb{F}(\sqrt{D})$ and $D_8$ otherwise.