Basic Theory of Field Extensions

Kevin James

Definition

The characteristic of a field F is defined to be the smallest integer p such that $p \cdot 1_F = 0_F$ is such p exists and 0 otherwise.

Definition

The characteristic of a field F is defined to be the smallest integer p such that $p \cdot 1_F = 0_F$ is such p exists and 0 otherwise.

Fact

If F is a field and $char(F) = p \neq 0$, then p is prime.

Definition

The characteristic of a field F is defined to be the smallest integer p such that $p \cdot 1_F = 0_F$ is such p exists and 0 otherwise.

Fact

If F is a field and $char(F) = p \neq 0$, then p is prime.

Definition

The prime subfield of a field F is the subfield generated by 1_F.

Definition

The characteristic of a field F is defined to be the smallest integer p such that $p \cdot 1_F = 0_F$ is such p exists and 0 otherwise.

Fact

If F is a field and $char(F) = p \neq 0$, then p is prime.

Definition

The prime subfield of a field F is the subfield generated by 1_F.

Fact

Suppose that F is a field and $L \subseteq F$ is its prime subfield. If $char(F) = 0$, then $L \cong \mathbb{Q}$. If $char(F) = p > 0$, then $L \cong \mathbb{F}_p$.

Definition

If K is a field containing the field F, then we say that K is an extension of F. We denote this by K/F or

$$\begin{array}{c} K \\ | \\ F \end{array}$$

Note that any field is an extension of its prime subfield. We sometimes say that the prime subfield is the base field of the extension.

Definition

If K is a field containing the field F, then we say that K is an extension of F. We denote this by K/F or

$$\begin{array}{c} K \\ | \\ F \end{array}$$

Note that any field is an extension of its prime subfield. We sometimes say that the prime subfield is the base field of the extension.

Definition

We define the degree of K/F denoted $[K : F]$ to be $\dim_F(K)$.

Proposition

Suppose that $\phi : F \to F'$ is a homomorphism of fields. Then ϕ is either identically 0 or injective.

Proposition

Suppose that $\phi : F \to F'$ is a homomorphism of fields. Then ϕ is either identically 0 or injective.

Theorem

Suppose that F is a field and that $p(x) \in F[x]$ is irreducible. Then $F[x]/(p(x))$ is an extension of F in which $p(x)$ has a root.

Proposition

Suppose that $\phi : F \to F'$ is a homomorphism of fields. Then ϕ is either identically 0 or injective.

Theorem

Suppose that F is a field and that $p(x) \in F[x]$ is irreducible. Then $F[x]/(p(x))$ is an extension of F in which $p(x)$ has a root.

Theorem

pose that F is a field and that $p(x) \in F[x]$ is irreducible with $\deg(p) = n$. Let $K = F[x]/(p(x))$ and let $\pi : F[x] \to K$ be the canonical projection homomorphism. Let $\theta = \pi(x) = x + (p(x))$. Then $\mathcal{B} = \{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a basis for K/F. Thus $[K : F] = n$.

Corollary

Let K and F be as in the previous theorem and let $a(\theta), b(\theta) \in K$. Then,

$$\begin{aligned} a(\theta) + b(\theta) &= (a+b)(\theta) \\ a(\theta)b(\theta) &= (ab)(\theta) = r(\theta), \end{aligned}$$

where $a(x)b(x) = p(x)q(x) + r(x)$ with $deg(r) < n$.

Definition

1. Suppose that K is an extension of F and $\{\alpha_i\}_{i\in I} \subseteq K$. The smallest subfield of K containing F and $\{\alpha_i\}_{i\in I}$ is denoted $F\left(\{\alpha_i\}_{i\in I}\right)$.
2. If $K = F(\alpha)$, then K is called a simple extension and α is called a primitive element of F.

Theorem

Suppose that $p(x) \in F[x]$ is irreducible and $K \supseteq F$ is an extension of F containing a root α of $p(x)$. Then $F(\alpha) \cong F[x]/(p(x))$.

Theorem

Suppose that $p(x) \in F[x]$ is irreducible and $K \supseteq F$ is an extension of F containing a root α of $p(x)$. Then $F(\alpha) \cong F[x]/(p(x))$.

Corollary

Suppose that $p(x) \in F[x]$ is irreducible with $\deg(p(x)) = n$ and $K \supseteq F$ is an extension of F containing a root α of $p(x)$. Then

$$F(\alpha) = \{\sum_{i=0}^{n-1} a_i \alpha^i \quad | \quad a_i \in F\} \subseteq K.$$

Theorem

Suppose that $p(x) \in F[x]$ is irreducible and $K \supseteq F$ is an extension of F containing a root α of $p(x)$. Then $F(\alpha) \cong F[x]/(p(x))$.

Corollary

Suppose that $p(x) \in F[x]$ is irreducible with $\deg(p(x)) = n$ and $K \supseteq F$ is an extension of F containing a root α of $p(x)$. Then

$$F(\alpha) = \{\sum_{i=0}^{n-1} a_i \alpha^i \quad | \quad a_i \in F\} \subseteq K.$$

Theorem

Let $\phi : F \to F'$ be an isomorphism and let $p(x) \in F[x]$ be irreducible. Let $\phi(p(x)) = p'(x) \in F'[x]$. Let α be a root of $p(x)$ in some extension K/F and let β be a root of $p'(x)$ in some extension K'/F'. Then there exists an isomorphism $\sigma : F(\alpha) \to F'(\beta)$ with $\sigma(\alpha) = \beta$ and $\sigma|_F = \phi$.