LECTURE 18

02.04.2024

(b) Suppose the characteristic of F is p. Then, $\ker f = p\mathbb{Z}$. Then we have, by first isomorphism theorem, $\frac{\mathbb{Z}}{p\mathbb{Z}} \cong \text{Image}(f)$. Here, $\text{Image}(f)$ is a subring of F with identity. But, $\text{Image}(f) \subseteq F$, and so $\text{Image}(f)$ is an integral domain. Then, $\text{Image}(f)$ is a finite integral domain and hence a field. $\text{Image}(f)$ is a subfield of F. and we have our $K \cong \text{Image}(f)$.

H.W. Show that $\mathbb{Q}$ and $\frac{\mathbb{Z}}{p\mathbb{Z}}$, for any prime p, are prime fields.

H.W. Let F be a field and let K be the intersection of all subfields of F. Show that K is a prime subfield of F.

Field extension

Let F be a field and K be a subfield of F. Then, we say, **F is an extension of K**. Let us denote this notion by F/K, and call it a **field extension**.

Now, take any $c \in F$. Then $K[c]$ is a subring of F with identity, in fact, an integral domain.

We define $K(c) = \{ab^{-1} \mid a, b \in K[c], b \neq 0\}$ as a quotient field of $K[c]$.

If we consider $c_1, c_2, \cdots, c_n \in F$, we can similarly construct:

$$K(c_1, c_2, \cdots, c_n) = K(c_1, c_2, \cdots, c_{n-1})(c_n).$$

We now introduce the concepts of **algebraic** and **transcendental** elements.

- Let F/K be a field extension. An element $a \in F$ is said to be **algebraic** over K, if there exist $k_0, k_1, \cdots, k_n \in K$, not all zero s.t. $k_0 + k_1 a + \cdots + k_n a^n = 0$. Otherwise, a is said to be **transcendental** over K.

Examples

- $\mathbb{R}/\mathbb{Q}$: $\sqrt{2}$ is algebraic over $\mathbb{Q}$

  $\mathbb{C}/\mathbb{R}$: i is algebraic over $\mathbb{R}$

  $\mathbb{C}/\mathbb{Q}$: i is algebraic over $\mathbb{Q}$

- $\mathbb{R}/\mathbb{Q}$: π, e are transcendental over $\mathbb{Q}$

  $F(x)/F$: x is transcendental over F.

H.W. Let F/K be a field extension. Then $c \in F$ is algebraic over K implies that c is a root of a unique irreducible monic polynomial $f(x)$ over K. (Also known as the minimal polynomial of c over K).

Theorem Let F/K be a field extension, and $c \in F$.

(A) if c is transcendental over K, then $K(c) \cong K(x)$, where $K(x)$ is the quotient

field of the polynomial ring $K[x]$.

(b) if c is algebraic over K, then $K[c] \cong \frac{K[x]}{(f(x))}$, where $f(x)$ is the minimal polynomial of c over K. [Check! $K(c) = K[c]$]

Proof. Given field K, we consider the polynomial ring $K[x]$ and a function $h : K[x] \to K[c]$, given by:
$h(g(x)) = g(c)$, for all $g(x) \in K[x]$.
Then, h is a surjective homomorphism from $K[x]$ to $K[c]$. So, we have:

$$\frac{K[x]}{\text{Ker } h} \cong K[c].$$

(a) if c is transcendental, $\text{Ker } h = \{0\}$, and hence, $K[x] \cong K[c]$, that is, h is an isomorphism. Then, h can be extended to an isomorphism $h^* : K(x) \to K(c)$ (Check!). Thus, $K(c) \cong K(x)$. This completes the proof.

(b) Suppose c is algebraic over K. Now, $\ker h$ is a principal ideal of $K[x]$. To show that $\ker h = (f(x))$.

We have that $\ker h = (g(x))$, where $g(x)$ is some monic polynomial of minimal degree. Then, $h(g(x)) = g(c) = 0$. So, c is a root of $g(x)$. Then, $f(x) \mid g(x)$. and so $(g(x)) \subseteq (f(x))$. Now, $f(c) = 0$, so, $f(x) \in \ker h$. Hence, $(f(x)) \subseteq (g(x))$. So, we have $(f(x)) = (g(x)) = \ker h$.

Fields as vector spaces

Let F/K be a field extension. Then, F can be considered as a vector space over K. The dimension of this vector space is denoted by $[F : K]$ and is said to be the degree of the extension F/K. If the dimension is finite, then F/K is called a finite extension; otherwise F/K is an infinite extension.

Theorem. Let F/K be a field extension and let $c \in F$ be algebraic over K. Let $f(x)$ be the minimal polynomial of c over K. If $\deg(f) = n$, then $\{1, c, c^2, \cdots, c^{n-1}\}$ forms a basis of the field extension $K(c)/K$.

Proof. Since c is algebraic over K, we have that $K(c) = K[c]$ (why?). We first show that $\{1, c, c^2, \cdots, c^{n-1}\}$ spans $K[c]$. Take any $g(c) \in K[c]$, with $g(x) \in K[x]$. Then considering $g(x)$ and $f(x)$, there exist polynomials $q(x)$ and $r(x)$, with $\deg(r) < \deg(f)$, s.t. $g(x) = q(x) \cdot f(x) + r(x)$. Then, $g(c) = q(c) f(c) + r(c) = r(c)$. This shows that $\{1, c, c^2, \cdots, c^{n-1}\}$ spans $K[c]$, in other words, the field extension $K(c)/K$. We now show that $\{1, c, c^2, \cdots c^{n-1}\}$ is linearly independent. Consider: $k_0 + k_1 c + \cdots + k_{n-1} c^{n-1} = 0$ with $k_i \in K$ for all i, with $0 \le i \le n-1$. If k_i's are not all zero, then c is a root

of a polynomial of degree $\leq n-1 < n$, a contradiction, and hence, all k_i's are zero.

So, $\{1, c, c^2, \cdots, c^{n-1}\}$ is linearly independent and hence forms a basis for the vector space $K(c)$ over K, that is, the field extension $K(c)/K$. This complete the proof.

Note: If c is algebraic over a field K, and degree of the minimal polynomial of c over K is n, then $[K(c) : K] = n$.

- We have seen transcendentals in a field extension, e.g., $\mathbb{R}/\mathbb{Q}$ where, π, e are transcendental elements over $\mathbb{Q}$. Now, $\mathbb{R}/\mathbb{Q}$ is an infinite field extension. Question: If we consider a finite field extension F/K would there exist elements in F that are transcendental over K?