Lecture: 15 - 16

[Home][PDF]

Topics: Conjugate elements,Automorphism and Traces

Conjugate elements with repect to a subfiled

In theorem 2.14 we saw that if $\alpha \in \mathbb{F}$ is a root of an irreducible polynomail f over $\mathbb{F}$ then all the roots of f are representeed by:

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$$

Theorem 2.14:

Irreducible poly in $\mathbb{F}[]$ of degree m has a root in $\mathbb{F}$.

To address elements of a field which are q-th powers of each other we introduced the notion of conjugates. (Def 2.17)

Two properties of conjugate elements giveen by 2.18 and Corollary 2.19

Prop: 2.18

The conjugates of $\alpha \in \mathbb{F_q}^$ with respect to any subfield $\mathbb{F_q}$ have the same order in the group $\mathbb{F_q}^$.

Proof:

Since $\mathbb{F_q}^$ is cyclic group by theorem 2.8, the result follows from Theorem 1.15(ii) and the fact that every power of charateristic of $\mathbb{F_q}$ is relatively privet to the order q-1 of $\mathbb{F_q}^$ $\square$

Corollary 2.19

Result at 2.18 if α is a primitive element of $\mathbb{F}$, then so are altso its conjugate with respect to any subfiled of $\mathbb{F}$

Exmample

Example of conjugate element in $\mathbb{F}_{\mathbf{16}}$ with respect to different subfields.

Let $\alpha \in \mathbb{F}_{\mathbf{16}}$ be an root of:

$$f(x) = x^4 + x + 1 \in \mathbb{F}_{\mathbf{2}}$$

Then the conjugate of α with respect to $\mathbb{F}_{\mathbf{2}}$ are:

$$\alpha, \alpha^2, \alpha^4 = \alpha + 1, \alpha^8 = \alpha^2 + 1$$

Each of them being a primitive element of $\mathbb{F}_{\mathbf{16}}$

The conjugates of α with respect to $\mathbb{F}_{\mathbf{4}}$ are α and $\alpha^4 = \alpha + 1$.

Automorphism for fields over a subfield

With automorphism σ of $\mathbb{F}$ over \mathbb{F_q}. We meawn automophisme that fixes an element of \mathbb{F_q}.

We then require that:

σ be a *one-to-one* mapping from $\mathbb{F}$ **onto** itself.

And the following holds:

$$\forall \alpha, \beta \in \mathbb{F}$$
$$\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta)$$
$$\sigma(\alpha\cdot\beta)=\sigma(\alpha)\cdot\sigma(\beta)$$
$$\sigma(a)=a, \forall a \in \mathbb{F}$$

Characterisation of all distinct automorphisms of $\mathbb{F}$ over $\mathbb{F}$

Definition 2.21

Distinct automiophism of $\mathbb{F}$ over $\mathbb{F}$ are exactly the mapping:

$$\sigma_0, \sigma_1, \sigma_2, .., \sigma_{m-1}$$

defineds by $\sigma_j(\alpha+\beta)=\sigma_j(\alpha)+\sigma_j(\beta)$ because of theorem 1.46, so that σ_j is an endomorphism of $\mathbb{F}$.

Further more $\sigma_j(\alpha)=0$ iff $\alpha=0$ and so σ_j is *one-to-one*. Since $\mathbb{F}$ is a finite set, σ_j is and epimorphism and therefor an automorphism of $\mathbb{F}$.

Moreover we have $\sigma_j(a)=a$ for all $a \in \mathbb{F}$ by lemma 2.3 and so each σ_j is and automophism of $\mathbb{F}$ over $\mathbb{F}$.

The mapping $\sigma_0, \sigma_1, \sigma_2, .., \sigma_{m-1}$ are distinct since they attain disctinct values for primitieve elements of $\mathbb{F}$

Now suppose that σ is an arbitraty automorphism of $\mathbb{F}$ over $\mathbb{F}_q}.

Let β be a primitive element (generator) of $\mathbb{F_{q^m}} and let

$$f(x)=x^m+a_{m-1}\cdot x^{m-1}+...+a_0 \in \mathbb{F}_{\mathbf{2}}[]$$

be its minimal polynomial over $\mathbb{F}$.

Then we have that:

$$0=\sigma(\beta^m+a_{m-1}\cdot\beta^{m-1}+...+a_0)$$
$$=\sigma(\beta^m)+a_{m-1}\cdot\sigma(\beta^{m-1})+...+a_0)$$

So that $\sigma(\beta)$ is a root of f in $\mathbb{F}$

It follows from Theorem 2.14 that: $\sigma(\beta)=\beta^{q^j}$ for some $j \in [0 \leq j \leq m-1]$

Since σ is a homomophism, we get that $\sigma(\alpha)=\alpha^{q^j}$ for all $\alpha \in \mathbb{F}$.

On the basis of 2.21, it is evident that conjugates of $\alpha \in \mathbb{F}$ with respect to $\mathbb{F}$ are obtainsed by applying all automophisms of $\mathbb{F}$ over $\mathbb{F}$ to element α.

The automorphism of $\mathbb{F}$ over $\mathbb{F}$ form a group with the operation being the usual composition of mappings.

The information provided in Theorem 2.21 shows that this gorup of automophisms of $\mathbb{F}$ over $\mathbb{F}$ is a cyclic group of order m generated by σ_1

Construction of irreducible ploynomials

An irreducible polynomial over $\mathbb{F}$ of degree n remains irreducible over $\mathbb{F}_k$ iff k and n are relative prime.

Relative prime: Two primes that don't divide eachother. **Coprime:** where you have common factors.

$$21=(1),(3),7,21$$
$$24=(1),2,(3),4,6,8,12,24$$

They share 1 and 3 as divisors, 21 and 24 are then *coprime*.

Example 1

Polynomial $x^2 + x + 1$ is irreducible over $\mathbb{F}_2$ degree 2 The it is irreducible over $\mathbb{F}_2$ is n is a odd number.

Example 2

Polynomial $x^3 + x + 1$ is irreducible over $\mathbb{F}_2$ degree 3 Then it is irreducible over $\mathbb{F}_2$ iff n is not dividible by 3.

Traces of elements of finite fields

Section 3, p50

In this section we adopt again the viewpoint of regarding $F = \mathbb{F}$ of the finite fields $K = \mathbb{F}$ as a vectorspace over K (Chapter 1, section 4).

Then F has dimentions m over K, and if $\{\alpha_1, \ldots, \alpha_m\}$ is a basis of F over K, each element $\alpha \in F$ can be uniquerly represented in the form:

$$\alpha = c_1 \cdot \alpha_1 + \ldots + c_m \cdot \alpha_m$$

with $c_j \in K$ for $1 \leq j \leq m$

We introduce an important mapping fraom $F \to K$ which will turn out to be linear.

Let $\alpha \in F$, Then the sum of all **conjugates** of α with respect to K is called "The trace of α over K" and is denoted by:

$$Tr_{F/K}(\alpha)$$

Definition 2.22

For $\alpha \in F = \mathbb{F}$ and $K = \mathbb{F}$

The trace of $Tr_{F/K}(\alpha)$ of α over K is defined by:

$$Tr_{F/K}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}$$

If K is a **prime subfield** of F then $Tr_{F/K}(\alpha)$ is called the **absoulute trace** of α and simply denoted $Tr_F(\alpha)$

In other words, the trace of α over K is the sum of all the conjugates of α with respect to K.

Still another description of the trace may be obtained as follows.

Let $f \in K[x]$ be the minimal polynomial of α over K. It's degree d is a divisor of m.

Then $g(x) = f(x)^{m/d} \in K$ is called the charateristic polynomial α over K.

By theorem 2.14, the roots of f in F are given by:

$$\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$$

And then a remark following 2.17 implies that the roots of g in F are precisley the conjucages of α with respect to K.

Hence:

$$g(x) = x^m + a_{m-1} \cdot x^{m-1} + \ldots + a_0$$

$$= (x - \alpha) \cdot (x - \alpha^q) \cdot \ldots \cdot (x - \alpha^{q^{m-1}}$$

And a comparison of coefficients show that:

$$Tr_{F/K}(\alpha) = -a_{m-1}$$

In particular, $Tr_{F/K}(\alpha)$ is always an element of K

Theorem 2.23 Holds all 5 properite sof the trace funtion.

Let $K = \mathbb{F}$ and $F = \mathbb{F}$ Then the trace function $Tr_{F/K}$ satifies the following properties:

i)

$$Tr_{F/K}(\alpha + \beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\alpha), \forall \alpha, \beta \in F$$

ii)

$$Tr_{F/K}(c \cdot \alpha) = c \cdot Tr_{F/K}(\alpha), \forall c \in K, \forall \alpha \in F$$

iii)

$Tr_{F/K}(\alpha)$ is linear tranformation from F **onto** K, when both F and K are viewed as vectospaces over K.

iv)

$$Tr_{F/K}(a) = m \cdot a, \forall a \in K$$

m is comming from $\mathbb{F}$

v)

$$Tr_{F/K}(\alpha^q) = Tr_{F/K}(\alpha), \forall \alpha \in \mathbb{F}$$

Where q is from $\mathbb{F}$

Proof (p.51)

Main takeway i) and ii) make iii) $Tr_{F/K}(\alpha)$ into a linear tranformation. It is sufficient to show that $\alpha \in F$ with $Tr_{F/K}(\alpha) \neq 0$

$Tr_{F/K}(\alpha) = 0$ iff α is a root of the polynomial:

- [x] \in F$$

But since this polynomial casn have at most q^{m-1} roots in F and F has q^m elements. We have are done, $F_{q^{m-1}} \neq F_{q^m} \square$

Theorem 2.25

Lef F be a finite extention of $K = \mathbb{F}$. Then for $\alpha \in F$ we have: $Tr_{F/K}(\alpha) = 0$ iff $\alpha = \beta^q - \beta$ for some $\beta \in F$.

Proof

Suppose $\alpha \in F = \mathbb{F}$ with $Tr_{F/K}(\alpha) = 0$ and let β be a root of $x^q - x - \alpha$ in some extension field of F. Then $\beta^q - \beta = \alpha$ and:

$$0 = Tr_{F/K}(\alpha)$$

$$RHS = \alpha + \alpha^q + .. + \alpha^{q^{q-1}}$$

$$= (\beta^q - \beta) + (\beta^q - \beta)^q + ... + (\beta^q - \beta)^{q^{m-1}}$$

$$= (\beta^q - \beta) + (\beta^{q^2} - \beta^q) + ... + (\beta^{q^m} - \beta^{q^{m-1}})$$

$$= (\beta^{q^m} - \beta)$$

$$\text{So that } \beta \in F$$

$$\square$$

Theorem 2.26 Transitivity of Trace

Let K be a finite field. Let F be a finite extension of K and E be a finite extendsion of F

$(K \subseteq F \subseteq E)$, K is the smallest field

$$Tr_{E/K}(\alpha) = Tr_{F/K}(Tr_{E/F}(\alpha)), \forall \alpha \in E$$

Proof is on page 53.

Basis of finite files over their subfields

Chapter 2, 3

If $F = \mathbb{F}$ and $K = \mathbb{F}$ then F can be viewed as an m dimentional vector space over K.

If $\alpha_1, \ldots, \alpha_m$ is a basis of F over K, then each element α in F can be uniquely represented on the form:

$$\alpha = c_1 \cdot \alpha_1, + \ldots + c_m \cdot \alpha_m$$

with $c_1, \ldots, c_m \in K$

There can be seceral different basis. There are tre particulare basis

- Dual basis
- Polynomial basis
- Normal basis

Definition 2.30 Dual basis

Let K be a finite field and F a finite extendion of K.

Then two bases {α, α_m } and { β, β_m } of F over K are said to be dual (complementary) bases if for $1 \leq i, j \leq m$:

$$Tr_{F/K}(\alpha_i \cdot \beta_j) = \{0, \text{for } i \neq j \; 1, \text{for } i = j$$

The dual basis is uniquely determind since its definition implies that the coefficient $c_j \alpha, 1 \leq j \leq m$ in 2.04 are given by:

$$c_j(\alpha) = Tr_{F/K}(\beta_j \cdot \alpha), \forall \alpha \in F$$

and by Theorem 2.24 the element $\beta_j \in F$ is uniquely determined by the linear trasformation c_j.

Definition 2.32 Normal basis

Let $K = \mathbb{F}$ and $F = \mathbb{F}$.

Then a basis of F over K on the form { $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$}.

Consists of a suitable element $\alpha \in F$ and its conjugate with respect to K is called the normal basis of F over K.

The basis { $\alpha, \alpha^2, 1 + \alpha + \alpha^2$} of $\mathbb{F}_8$ over $\mathbb{F}_2$

Is a normal basis of $\mathbb{F}_8$ over $\mathbb{F}_2$ since $1 + \alpha + \alpha^2 = \alpha^4$.

Definition: Polybasis

A basis F over K of the form:

$$1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$$

with α defining element of F over K.

That is $F = K(\alpha)$ is called a polynomial basis.

If α is a primitice element of F then $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ os a polynomial basis.

Example 2.31

Let $\alpha \in \mathbb{F}_{\mathbf{8}}$ be a root of the irreducivble polynomial

$$x^3 + x^2 + 1 \in \mathbb{F}_{\mathbf{2}}[]$$

Then $\mathbb{F}_{\mathbf{8}} = \mathbb{F}_{\mathbf{2}}(\alpha)$ and $1, \alpha, \alpha^2, \alpha^3$ is a polynomial basis

On the other hand $1, \alpha, \alpha^2, 1 + \alpha + \alpha^2$ is a basis dual to itself and it si also a normal basis over $\mathbb{F}_{\mathbf{2}}$

Since $1 + \alpha + \alpha^2 = \alpha^4$,

then $1, \alpha, \alpha^2, 1 + \alpha + \alpha^2$ is a normal basis over $\mathbb{F}_{\mathbf{2}}$