Abstract Algebra by Pinter, Chapter 29

Amir Taaki

Abstract

Chapter 29 on Degress of Field Extensions

Contents

1 A. Examples of Finite Extensions

1.1 Q1

$x^2 + 2$ has root $i\sqrt{s}$

$$[\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}] = 2$$
$$\mathbb{Q}(i\sqrt{2}) = \{a + bi\sqrt{2}\}$$

1.2 Q2

$$x = 2 + 3i$$
$$(x-2)^2 = -9$$
$$x^2 - 4x + 13 = 0$$
$$\{a, bi\}$$

1.3 Q3

$$a = \sqrt{1 + \sqrt[3]{2}}$$
$$a^2 + 1 = \sqrt[3]{2}$$
$$a^2 + 1 \in \mathbb{Q}(a) \implies \sqrt[3]{2} \in \mathbb{Q}(a)$$
$$x = \sqrt[3]{2}$$
$$\therefore x^3 - 2 = 0$$
$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

Basis for $\mathbb{Q}(\sqrt[3]{2})$ is $\{1, 2^{\frac{1}{3}}, 2^{\frac{1}{3}}\}$

$$a^2 + (1 - \sqrt[3]{2}) = 0$$
$$\sqrt[3]{2} \in \mathbb{Q}(a) \implies \mathbb{Q}(a) = \mathbb{Q}(a, \sqrt[3]{2})$$
$$[\mathbb{Q}(a) : \mathbb{Q}(\sqrt[3]{2})] = 2$$

Basis for $\mathbb{Q}(a)$ over $\mathbb{Q}(\sqrt[3]{2})$ is $\{1, a\}$. Thus basis for $\mathbb{Q}(a)$ over $\mathbb{Q}$ is the products:

$$\{1, 2^{1/3}, 2^{2/3}, a, 2^{1/3}a, 2^{2/3}a\}$$

1.4 Q4

$$a = \sqrt{2} + \sqrt[3]{4}$$
$$(a - \sqrt[3]{4})^2 = 2$$
$$a^2 - 2\sqrt[3]{4} + 4^{2/3} - 2 = 0$$
$$a^2 = 2 + 2 \cdot 4^{1/3} - 4^{2/3}$$
$$a^2 \in \mathbb{Q}(\sqrt{2} + \sqrt[3]{4}) \implies 4^{1/3} \in \mathbb{Q}(\sqrt{2} + \sqrt[3]{4})$$
$$x = \sqrt[3]{4}$$
$$\therefore x^3 - 4 = 0$$
$$[\mathbb{Q}(4^{\frac{1}{3}}) : \mathbb{Q}] = 3$$

Basis is $\{1, 4^{\frac{1}{3}}, 4^{\frac{2}{3}}\}$. From earlier $a^2 = 2 + 2 \cdot 4^{\frac{1}{3}} - 4^{\frac{2}{3}}$ so $[\mathbb{Q}(\sqrt{2} + \sqrt[3]{4}) : \mathbb{Q}(4^{\frac{1}{3}})] = 2$.

Note that $4^{\frac{1}{3}} \notin \mathbb{Q}(2^{\frac{1}{2}})$, otherwise $4^{1/3} = a + b2^{\frac{1}{2}}$ which is impossible, since squaring both sides would lead to a contradiction. So $\mathbb{Q}(2^{\frac{1}{2}}) = \mathbb{Q}(2^{\frac{1}{2}}, 4^{\frac{1}{3}})/$

Basis for $\mathbb{Q}(2^{\frac{1}{2}} + 4^{\frac{1}{3}})$

$$\{1, 4^{\frac{1}{3}}, 4^{\frac{2}{3}}, 2^{\frac{1}{2}}, 4^{\frac{1}{3}}2^{\frac{1}{2}}, 4^{\frac{2}{3}}2^{\frac{1}{2}}\}$$

1.5 Q5

$$x^2 - 5 = 0 \implies [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$$

Let $\sqrt{7} \in \mathbb{Q}(\sqrt{5})$, then

$$\sqrt{7} = a + b\sqrt{5} : a, b \in \mathbb{Q}$$

Squaring both sides we have

$$7 = a^2 + 2ab\sqrt{5} + 5b^2$$

This is a contradiction since re-arranging terms would mean $\sqrt{5} \in \mathbb{Q}$ and hence a rational number for $a, b \neq 0$. If $b = 0$, then $\sqrt{7} = a$ which is rational and if $a = 0$ then $\sqrt{7} = b\sqrt{5}$ or $\sqrt{7} \cdot \sqrt{5} = 5b$, again a contradiction.

$$\implies \sqrt{7} \notin \mathbb{Q}(\sqrt{5})$$

$$x^2 - 7 = 0 \implies [\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = 2$$
$$\implies \mathbb{Q}(\sqrt{5}, \sqrt{7}) = \{a + b\sqrt{5} + c\sqrt{7} + d\sqrt{35} : a, b, c, d \in \mathbb{Q}\}$$

1.6 Q6

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = \{a\sqrt{2} + b\sqrt{3} + c\sqrt{5} + d\sqrt{6} + e\sqrt{10} + f\sqrt{15} : a, b, c, d, e, f \in \mathbb{Q}\}$$

1.7 Q7

π is algebraic meands it is the root of some polynomial in the field. Of degree 3 means the polynomial has degree 3 which is also the degree of the field.

Suppose $\pi \in \mathbb{Q}(\pi^3)$, then

$$\pi = a + b\pi^3$$

but this is impossible since π is transcendental over $\mathbb{Q}$ and $\pi \neq \pi^3$.

This π is algebraic over $\mathbb{Q}(\pi^3)$ with

$$x^3 - \pi^3 = 0$$

$$\mathbb{Q}(\pi) = \mathbb{Q}(\pi^3, \pi)$$
$$x^3 - \pi^3 \in \mathbb{Q}(\pi^3)[x]$$

2 B. Further Examples of Finite Extensions

2.1 Q1

$$\sqrt{a} + \sqrt{b} \in F$$
$$a + 2\sqrt{a}\sqrt{b} + b \in F$$
$$\text{char } F \neq 2 \implies 2\sqrt{a}\sqrt{b} \neq 0$$
$$\implies 2\sqrt{a}\sqrt{b} \in F \implies \sqrt{a}\sqrt{b} \in F$$

$$\sqrt{ab}(\sqrt{a} + \sqrt{b}) = a\sqrt{b} + b\sqrt{a} \in F$$
$$b(\sqrt{a} + \sqrt{b}) = b\sqrt{b} + b\sqrt{a} \in F$$

$$(a\sqrt{b}+b\sqrt{a})-(b\sqrt{b}+b\sqrt{b})=(a-b)\sqrt{b}\in F$$
$$\implies \sqrt{b}\in F$$

Likewise for $\sqrt{a}$.

$$\sqrt{a}+\sqrt{b}\in F(\sqrt{a},\sqrt{b})$$
$$\sqrt{a},\sqrt{b}\in F(\sqrt{a}+\sqrt{b})$$
$$\implies F(\sqrt{a},\sqrt{b})=F(\sqrt{a}+\sqrt{b})$$

2.2 Q2

$$F(\sqrt{a})=\{x+y\sqrt{a}:x,y\in F\}$$
$$\sqrt{b}\in F(\sqrt{a})$$
$$\sqrt{b}=x+y\sqrt{a}$$
$$b=x^2+2xy\sqrt{a}+y^2a$$

which implies $\sqrt{a}$ is rational, a contradiction.

$$\sqrt{b}\notin F(\sqrt{a})$$

$$\begin{aligned}\implies [F(\sqrt{a},\sqrt{b}):F]&=[F(\sqrt{a},\sqrt{b}):F(\sqrt{a})][F(\sqrt{a}):F]\\&=[F(\sqrt{b}):F][F(\sqrt{a}:F]\\&=4\end{aligned}$$

2.3 Q3

Use sage.

2.4 Q4

$$a+b=7$$
$$a=7-b$$
$$(a-b)^2=(7-2b)^2=9$$
$$7-2b=\pm 3$$
$$2b=10,4$$
$$b=5,2$$
$$a=2,5$$
$$\mathbb{Q}(\sqrt{2},\sqrt{5})$$
$$\{1,\sqrt{2},\sqrt{5}\}$$

3 C. Finite Extensions of Finite Fields

3.1 Q1

$$a(x)=p(x)q(x)+r(x)$$

where $r(x)=0$ or $\deg r(x)<\deg b(x)$

$$\forall a(x)\in F[x], a(x)=p(x)q(x)+r(x)$$

$$\implies \langle p(x)\rangle + a(x)=\langle p(x)\rangle + r(x)$$

$\deg r(x)<n$ and $F[x]/\langle p(x)\rangle\cong F(c)$

3.2 Q2

$p(x) = x^2 + x + 1$ is irreducible because $p(0) = 1$ and $p(1) = 1$.

Quotient field formed by $p(x)$ consists of all 1 degree polynomials of the form $a_0 + a_1 x$, where $a_i \in \mathbb{Z}_2$.

There is a c st $p(c) = 0$, and

$$\mathbb{Z}_2(c) \cong \mathbb{Z}_2[x]/\langle p(x) \rangle$$

$$\begin{aligned} p(c) &= c^2 + c + 1 = 0 \\ \implies c^2 &= c + 1 \end{aligned}$$

+	0	1	c	c + 1
0	0	1	c	c + 1
1	1	0	c + 1	c
c	c	c + 1	0	1
c + 1	c + 1	c	1	0

×	0	1	c	c + 1
0	0	0	0	0
1	0	1	c	c + 1
c	0	c	c + 1	1
c + 1	c + 1	c	1	c

3.3 Q3

$$p(x) = x^3 + x^2 + 1$$

$p(0) = 1, p(1) = 1 \implies p(x)$ is irreducible and has no roots in $\mathbb{Z}_2$. $\deg p(x) = 3 \implies B = \{1, x, x^2\}$

Let there be a c such that $p(c) = $, then $\mathbb{Z}_2(c) \cong \mathbb{Z}_2[x]/\langle p(x) \rangle$.

3.4 Q4

a is algebraic over F of degree n

$$\implies F(a) = \{a_0 + \cdots + a_{n-1}x^{n-1} : a_i \in F\}$$

There are q possible values for $a_0, a_1, \ldots, a_{n-1}$ each and so $|\{(a_0, \ldots, a_{n-1}) : a_i \in F\}| = q^n$

$$\implies |F(a)| = q^n$$

3.5 Q5

Let $p(x) = x^2 - k$ where $k \in \mathbb{Z}_p$ then if $p(x)$ is reducible then $c^2 = k$.

From 23H, let $h : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ be defined by $h(\overline{a}) = \overline{a}^2$, then the range of h has $(p-1)/2$ and so is non-injective and non-surjective.

This means there exists $k \in \mathbb{Z}_p$, such that there is no $c \in \mathbb{Z}_p : c^2 = k$, and so $p(x) = x^2 - k$ has no roots in $\mathbb{Z}_p$.

4 D. Degrees of Extensions

4.1 Q1

K forms an extension field over F with basis of dimension 1 $\iff K = F$.

4.2 Q2

$L \subset K \implies \dim L < \dim K$.

Dimensions cannot be the same or that would imply they are the same.

So L divides the order of K.

$$[K : F] = [K : L][L : F]$$

But $[K : F]$ is prime so L cannot exist.

4.3 Q3

$$a \in K - F \implies [F(a) : F] \leq [K : F]$$

But there are subfields of K except F since the extension order is prime so $K = F(a)$.

4.4 Q4

4.4.1 a

$$F(a, b) = (F(a))(b)$$

$$\begin{aligned}[F(a, b) : F] &= [F(a, b) : F(a)][F(a) : F] \\ &= [F(a, b) : F(a)] \cdot m\end{aligned}$$

However $[F(b) : F] = n$ so $[F(a, b) : F] = [F(a, b) : F(b)][F(b) : F] = n$ Thus $[F(a, b)] = mx = ny$ and $\gcd(m, n) = 1 \implies [F(a, b) : F] = mn$.

4.4.2 b

$$K \subseteq F(a), F(b) : K = F(a) \cap F(b)$$
$$[F(a) : F] = [F(a) : K][K : F]$$
$$[F(b) : F] = [F(b) : K][K : F]$$

$$\frac{m}{n} = \frac{[F(a) : K]}{[F(b) : K]}$$

Since $\gcd(m, n) = 1$, m and n share no divisors, and so they cannot be reduced.

But $[F(a) : F] = m$ and $[F(b) : F] = n$ so this means $[F(a) : K] = m, [F(b) : K] = n$ and since $[F(a) : F] = m$, so $K = F$.

4.5 Q5

The extension is finite and algebraic, so any $a \in F(a)$ forms a subfield of $F(a)$.

But $F(a)$ has no subfields so $F(a^n) = F(a)$.

4.6 Q6

$$\begin{aligned}p(a) = 0 &\implies L = F(a) \subseteq K \\ &\implies \deg p(x) = [L : F]\end{aligned}$$

But,

$$\begin{aligned}[K : F] &= [K : L][L : F] \\ &= [K : L] \cdot \deg p(x)\end{aligned}$$

$$\deg p(x) | [K : F]$$

5 E. Short Questions Relating to Degrees of Extensions

5.1 Q1

$$\frac{1}{a} \in F(a) \text{ and } a \in F(\frac{1}{a}) \implies F(a) = F(\frac{1}{a})$$

$p(x)$ is the minimum polynomial for a, then substitute $a + c$ or ac and the degree of the polynomial doesn't change.

5.2 Q2

$$p(x) = x - a, \deg p(x) = 1$$

5.3 Q3

If $c \in \mathbb{Q}$, then $\deg p(x) = 1$, thus

$$\deg p(x) > 1 \implies c \notin \mathbb{Q}$$

5.4 Q4

$$b(c) = x^2 - \frac{m}{n} = 0$$
$$p \mid m, p^2 \nmid m \implies b(x) \text{ is irreducible}$$
$$\implies \sqrt{m/n} \notin \mathbb{Q}$$

5.5 Q5

$$b(x) = x^q - \frac{m}{n}$$

and Eisenstein's criteria still holds.

5.6 Q6

$F(a)$ is a finite extension of F, and $F(a, b)$ is a finite extension of $F(a)$.

$(r \cdot s)(x) = r(x)s(x)$, $(r \cdot s)(a) = 0$ and $(r \cdot s)(b) = 0$, so $F(a, b)$ is a finite extension of F since the degree of $r \cdot s$ is finite.

6 F. Further Properties of Degrees of Extensions

6.1 Q1

K is a finite extension of F, so all elements of K are also algebraic over F. So all algebraic extensions of K are also finite algebraic extensions of F.

$$[K(a) : F] = [K(a) : K][K : F]$$

6.2 Q2

$$[K(a) : F] = [K(b) : F(b)][F(b) : F]$$
$$\implies [F(b) : F] \mid [K(b) : F]$$

6.3 Q3

$$p(x) = a_0 + \cdots + a_{n-1}x^{n-1}, a_i \in F$$

$p(b) = 0$ over F. Let minimum polynomial of K be $q(x)$ then

$$p(x) = s(x)q(x) + r(x)$$

therefore minimum polynomial for b over K is $r(x)$ and $\deg r(x) \leq \deg p(x)$

$$\implies [K(b) : K] \leq [F(b) : F]$$

6.4 Q4

$$[K(b) : K] \leq [F(b) : F]$$
$$[K(b) : F] = [K(b) : K][K : F]$$
$$[K(b) : F] = [K(b) : F(b)][F(b) : F]$$
$$\implies [K(b) : K][K : F] = [K(b) : F(b)][F(b) : F]$$

But $[K(b) : K] \leq [F(b) : F]$

$$\implies [K : F] \geq [K(b) : F(b)]$$

6.5 Q5

The degree of the minimum polynomial does not divide the degree of $p(x)$, so when applying polynomial long division there will be a remainder left over, which $p(x)$ itself. So $p(x)$ is not divided by $q(x)$.

7 G. Fields of Algebraic Elements: Algebraic Numbers

7.1 Q1

$F(a, b)$ is algebraic extension, and $a + b, a - b, ab, a/b \in F(a, b)$

7.2 Q2

Every element of the set forms a closed field over F, so the set is a subfield of K which contains F.

7.3 Q3

All the coefficients belong to $\mathbb{A}$ which are algebraic over $\mathbb{Q}$ and hence form a finite extension of $\mathbb{Q}$.

7.4 Q4

$\mathbb{Q}_1(c)$ is a finite extension of $\mathbb{Q}_1$ and $\mathbb{Q}_1$ is a finite extension of $\mathbb{Q} \implies \mathbb{Q}_1(c)$ is a finite extension of $\mathbb{Q}$.

7.5 Q5

c is the root of a finite polynomial whose coefficients are in finite extensions of $\mathbb{Q}$, and so c forms a finite extension over $\mathbb{Q} \implies c \in \mathbb{A}$.