

Abstract Algebra by Pinter, Chapter 31

Amir Taaki

Chapter 31 on Galois Theory Preamble

Contents

A. Examples of Root Fields over \mathbb{Q}	2
Q1	2
Q2	2
Q3	3
Q4	3
Q5	3
Q6	3
B. Examples of Root Fields over \mathbb{Z}_p	4
Q1	4
Q2	4
Q3	5
Q4	6
Q5	6
C. Short Questions Relating to Root Field	7
Q1	7
Q2	7
Q3	7
Q4	8
Q5	8
Q6	8
Q7	8
Q8	8
Q9	9
D. Reducing Iterated Extensions to Simple Extensions	9
Q1	9
a	9
b	9
Q2	9
Q3	9
Q4	10
Q5	10
E. Roots of Unity and Radical Extensions	10
Q1	10
Q2	10
Q3	11
Q4	11
n = 6	11
n = 7	11
n = 8	11
Q5	11
Q6	12
Q7	12
Q8	12

F. Separable and Inseparable Polynomials	12
Q1	12
Q2	12
Q3	12
Q4	12
Q5	13
Q6	13
Q7	13
G. Multiple Roots over Infinite Fields of Nonzero Characteristic	13
Q1	13
Q2	13
Q3	13
Q4	13
Q5	13
H. An Isomorphism Extension Theorem (Proof of Theorem 3)	14
Q1	14
Q2	14
Q3	14
Q4	14
Q5	14
I. Uniqueness of the Root Field	15
Q1	15
Q2	15
Q3	15
$F_1(u) = K_1$	16
$F_1(u) \neq K_1$	16
$\deg a(x) = 1$	16
Q4	16
J. Extending Isomorphism	16
Q1	16
Q2	17
Q3	17
Q4	17
Q5	17
K. Normal Extensions	18
Q1	18
Q2	18

Note that root field is called splitting field in other texts.

A. Examples of Root Fields over \mathbb{Q}

Q1

```
sage: solve(x^2 - 2*x - 2, x)
[x == -sqrt(3) + 1, x == sqrt(3) + 1]
sage: solve(x^2 + 1, x)
[x == -I, x == I]
```

Q2

Possible roots for $x^2 - 3$ are $\pm 1, \pm 3$.

```
sage: p = lambda x: x^2 - 3
sage: p(-1), p(1), p(-3), p(3)
(-2, -2, 6, 6)
```

So it is irreducible.

For $x^2 - 2x - 2$ we can use Eisenstein's irreducibility criteria.

```
sage: solve(x^2 - 3, x)
[x == -sqrt(3), x == sqrt(3)]
sage: solve(x^2 - 2*x - 2, x)
[x == -sqrt(3) + 1, x == sqrt(3) + 1]
```

Root field is $\mathbb{Q}(\sqrt{3})$.

Q3

```
sage: solve(x^4 - 2, x)
[x == I*2^(1/4), x == -2^(1/4), x == -I*2^(1/4), x == 2^(1/4)]
```

Therefore the root field is $\mathbb{Q}(2^{1/4}, i)$

Since $\mathbb{Q}(2^{1/4}) \subseteq \mathbb{R}$, then the root field of $x^4 - 2$ over \mathbb{R} is $\mathbb{R}(i)$.

Q4

```
sage: solve(x^4 - 2*x^2 + 9, x)
```

```
[x == -sqrt(2*I*sqrt(2) + 1), x == sqrt(2*I*sqrt(2) + 1), x == -sqrt(-2*I*sqrt(2) + 1), x == sqrt(-2*I*sqrt(2) + 1)]
```

Root field is $\mathbb{Q}(i, \sqrt{2})$.

```
sage: solve(x^2 - 2*sqrt(2)*x + 3, x)
[x == sqrt(2) - I, x == sqrt(2) + I]
```

Root field is $\mathbb{Q}(i, \sqrt{2})$.

Q5

```
sage: c
sqrt(3) + I
sage: ((c^2 - 2)^2).expand()
-12
```

```
sage: ((x^2 - 2)^2)
....: ).expand()
```

```
x^4 - 4*x^2 + 4
```

```
sage: x^4 - 4*x^2 + 4 + 12
x^4 - 4*x^2 + 16
```

```
sage: solve(x^4 - 4*x^2 + 4 + 12, x)
```

```
[x == -sqrt(2*I*sqrt(3) + 2), x == sqrt(2*I*sqrt(3) + 2), x == -sqrt(-2*I*sqrt(3) + 2), x == sqrt(-2*I*sqrt(3) + 2)]
```

So there are roots $-2\sqrt{3}i - 2$ and $2\sqrt{3}i - 2$.

And $x^2 - 3$ for $b(x)$.

```
sage: c = sqrt(2) + sqrt(3)
sage: (c^2).expand()
2*sqrt(3)*sqrt(2) + 5
sage: (((c^2).expand() - 5)^2).expand()
24
```

```
sage: ((x^2 - 5)^2).expand()
```

```
x^4 - 10*x^2 + 25
```

```
sage: solve(x^4 - 10*x^2 + 1, x)
```

```
[x == -sqrt(2*sqrt(6) + 5), x == sqrt(2*sqrt(6) + 5), x == -sqrt(-2*sqrt(6) + 5), x == sqrt(-2*sqrt(6) + 5)]
```

Remembering that $\sqrt{6} = \sqrt{2}\sqrt{3}$.

Q6

All of them are valid root fields except the cube root one.

B. Examples of Root Fields over \mathbb{Z}_p

Q1

```
sage: R.<x> = IntegerModRing(3) []
sage: f = x^3 + 2*x + 1
sage: S.<u> = R.extension(f)
sage: (x - u)*(x - (u + 1))*(x - (u + 2))
x^3 + 2*x + 1
```

List the elements:

```
sage: S = R.quotient(x^3 + 2*x + 1, 'u')
sage: len(S)
27
sage: list(S)
[0,
 1,
 2,
 u,
 u + 1,
 u + 2,
 2*u,
 2*u + 1,
 2*u + 2,
 u^2,
 u^2 + 1,
 u^2 + 2,
 u^2 + u,
 u^2 + u + 1,
 u^2 + u + 2,
 u^2 + 2*u,
 u^2 + 2*u + 1,
 u^2 + 2*u + 2,
 2*u^2,
 2*u^2 + 1,
 2*u^2 + 2,
 2*u^2 + u,
 2*u^2 + u + 1,
 2*u^2 + u + 2,
 2*u^2 + 2*u,
 2*u^2 + 2*u + 1,
 2*u^2 + 2*u + 2]
```

Roots of $a(x)$ are $u, u + 1, u + 2$.

Root field is therefore $\mathbb{Z}_3(u)$.

Q2

```
sage: S = R.quotient(x^2 + x + 2, 'u')
sage: list(S)
[0, 1, 2, u, u + 1, u + 2, 2*u, 2*u + 1, 2*u + 2]
```

Utilize the fact that $u^2 = -u - 2 = 2u + 1$, we can make the addition and multiplication tables.

```
sage: from sage.matrix.operation_table import OperationTable
sage: OperationTable(S, operation=operator.add)
+-----+
| a b c d e f g h i
b| b c a e f d h i g
c| c a b f d e i g h
d| d e f g h i a b c
```

```

e| e f d h i g b c a
f| f d e i g h c a b
g| g h i a b c d e f
h| h i g b c a e f d
i| i g h c a b f d e

sage: OperationTable(S, operation=operator.mul)
* a b c d e f g h i
+-----
a| a a a a a a a a a
b| a b c d e f g h i
c| a c b g i h d f e
d| a d g h b e f i c
e| a e i b f g c d h
f| a f h e g c i b d
g| a g d f c i h e b
h| a h f i d b e c g
i| a i e c h d b g f

```

Roots are: $u, 2u + 2$ (figured by substitution)

Root field: $\mathbb{Z}_3(u)$

Q3

Root field will be all combos of polynomials over \mathbb{Z}_2 of degree 2 polynomials.

```

sage: R.<x> = IntegerModRing(2) []
sage: S = R.quotient(x^3 + x^2 + 1, 'u')
sage: list(S)
[0, 1, u, u + 1, u^2, u^2 + 1, u^2 + u, u^2 + u + 1]

```

In \mathbb{Z}_2 , $-1 = 1$ so $u^3 = u^2 + 1$.

```

sage: OperationTable(S, operation=operator.add)
+ a b c d e f g h
+-----

```

```

a| a b c d e f g h
b| b a d c f e h g
c| c d a b g h e f
d| d c b a h g f e
e| e f g h a b c d
f| f e h g b a d c
g| g h e f c d a b
h| h g f e d c b a

```

```

sage: OperationTable(S, operation=operator.mul)
* a b c d e f g h
+-----

```

```

a| a a a a a a a a
b| a b c d e f g h
c| a c e g f h b d
d| a d g f b c h e
e| a e f b h d c g
f| a f h c d g e b
g| a g b h c e d f
h| a h d e g b f c

```

```

sage: R.<x> = IntegerModRing(2) []

```

```

sage: f = x^3 + x^2 + 1

```

```

sage: S.<u> = R.extension(f)

```

```

...

```

```

sage: f(u)

```

```

0

```

```

sage: f(u^2)
0
sage: f(u^2 + u + 1)
0
sage: (x - u)*(x - u^2)*(x - (u^2 + u + 1))
x^3 + x^2 + 1
Root field:  $\mathbb{Z}_3(u)$ 

```

Q4

```

sage: f = x^3 + x + 1
sage: S.<u> = R.extension(f)
sage: f(u)
0
sage: f(u + 1)
u^2 + u
sage: f(u^2)
0
sage: f(u^2 + 1)
u
sage: f(u^2 + u)
0
sage: f(u^2 + u + 1)
u^2

```

Roots are $u, u^2, u^2 + u$.

Q5

```

sage: R.<x> = IntegerModRing(3) []
sage: f = x^3 + x^2 + x + 2
sage: S.<u> = R.extension(f)
sage: f(u)
0
sage: f(u + 1)
2*u
sage: f(u + 2)
u + 2
sage: f(u^2)
u^2
sage: f(u^2 + 1)
0
sage: f(u^2 + 2)
2*u^2 + 2
sage: f(u^2 + u)
2*u^2 + u
sage: f(u^2 + u + 1)
u^2
sage: f(u^2 + 2*u)
2*u^2 + 2*u
sage: f(u^2 + 2*u + 1)
u^2
sage: f(u^2 + u + 2)
2*u + 2
sage: f(u^2 + 2*u + 2)
u + 2
sage: f(2*u)
2*u^2 + 1
sage: f(2*u + 1)
2*u^2 + u + 1
sage: f(2*u + 2)

```

```

2*u^2 + 2*u
sage: f(2*u^2)
2*u^2 + u + 2
sage: f(2*u^2 + 1)
u + 2
sage: f(2*u^2 + 2)
u^2 + u + 1
sage: f(2*u^2 + u)
u^2 + 1
sage: f(2*u^2 + 2*u)
2*u^2 + 2*u
sage: f(2*u^2 + u + 1)
2*u^2 + 2*u + 1
sage: f(2*u^2 + u + 2)
u
sage: f(2*u^2 + 2*u + 1)
0

```

I think the answer in the book is wrong since

```

sage: R.<x> = IntegerModRing(3) []
sage: f = x^3 + x^2 + x + 2
sage: S.<u> = R.extension(f)
sage: u^3 + u^2 + u + 2
0
sage: f(u^2 + 1)
0
sage: f(2*u^2 + 2*u + 1)
0
sage: (x - u)*(x - (u^2 + 1))*(x - (2*u^2 + 2*u + 1))
x^3 + x^2 + x + 2

```

We can even substitute these roots into $q(x)$ which is claimed to be irreducible

```

sage: a = lambda x: (x^2 + (u + 1)*x + (u^2 + u + 1))
sage: a(u^2 + 1)
0
sage: a(2*u^2 + 2*u + 1)
0

```

Roots are: $u, u^2 + 1, 2u^2 + 2u + 1$.

Basis is $\{u^2, u, 1\}$.

C. Short Questions Relating to Root Field

Q1

The basis for a degree 2 extension $\mathbb{F}(c)$ is $\{c, 1\}$ with $c^2 \in \mathbb{F}$. This includes $-c$ and so $\mathbb{F}(c)$ is the root field for $(x + c)(x - c) = x^2 - c^2$.

The question I assume is asking to prove every degree 2 field extension is [normal](#). So since $c \in F(c)$, then we can divide the polynomial by $(x - c)$, leaving a degree 1 polynomial $(x - \alpha) \in F(c)[x]$ or that $\alpha \in F(c)$.

Q2

$a(x)$ as a polynomial of degree n over a finite field will have n distinct roots. All roots $c_1, \dots, c_n \in K$ and form a root field over F . Assume some roots are in I , then the roots of $a(x)$ are still the same, and so K forms a root field over I as well.

Q3

Any polynomial can be factored into a linear combination of complex roots. This means \mathbb{C} is the root field of every polynomial. Since polynomials can also have root fields contained in \mathbb{R} , and $\mathbb{R} \subset \mathbb{C}$, this means the root

field is either \mathbb{R} or \mathbb{C} of every polynomial.

Q4

This question is impossible. See the answer [here](#).

Q5

As per the back of the book, we just need to show that $F(d_1, d_2) = F(c)$ and that it's the splitting field.

$$\begin{aligned}d_1^2 &= \frac{a^2}{4} - b \\d_2^2 &= \frac{a}{2} + d_1 \\&= \frac{a}{2} + \sqrt{\frac{a^2}{4} - b}\end{aligned}$$

Roots of $p(x)$ are $\pm\sqrt{\frac{a}{2} \pm d_1}$. We know that $\frac{a}{2} \pm d_1 \in F(d_1)$.

$[F(d_1) : F] = 2$. Every extension of degree 2 is a root field from 31C1 above.

Q6

$$\sigma_c(a(x)) = a(c)$$

$$\ker \sigma_c = \{a(x) : a(c) = 0\}$$

Every ideal of a field [is principal](#), so $J = \langle p(x) \rangle$. For some $a(x) \in J$, $a(x)$ is a multiple of $p(x)$.

$$\sigma_c : F[x] \rightarrow F$$

so $F(c)$ contains $p(x)$ since the ideal J contains all polynomials with c as their root, and all polys are a multiple of $p(x)$.

Q7

From the previous argument $p(x)$ is the lowest degree polynomial in J and hence irreducible. Otherwise $p(c) = f(c)g(c) = 0 \implies f(c) = 0$ or $g(c) = 0$ which would be a contradiction since it implies there would be a lower degree polynomial in J . Every root field is a simple extension $F(c)$, we can convert a polynomial with roots a, b to one with c from theorem 2 in this chapter.

Q8

Give an isomorphism $h(x)$ which fixes F , and a polynomial

$$a(x) = a_0 + a_1x + \cdots + a_nx^n$$

We can see that where c is an algebraic root in K , then

$$\begin{aligned}a(h(c)) &= a_0 + a_1h(c) + \cdots + a_nh(c^n) \\&= h(a(c)) = h(0) = 0\end{aligned}$$

So also $h(c)$ is a root of $a(x)$ and the isomorphism simply permutes roots since it sends unique elements of K to K' . We also observe that the mapping is one to one, fixing F , permuting roots, and that $h : K \rightarrow K$.

$$h(\{c_1, \dots, c_n\}) = \{c_1, \dots, c_n\}$$

Since the polynomial $a(x)$ is irreducible over F , and K being a finite extension can be reduced to a simple extension $F(c) = K$, where c is a root of $a(x)$, which means that

$$F(c) \cong F/\langle a(x) \rangle$$

which forms a vector space of $\deg a(x) = n \implies [K : F] = n$.

Given another polynomial $b(x)$ where $b(c) = 0 : c \in K \implies b(h(c)) = 0 \implies K$ is the splitting field for $b(x)$. This means $b(x)$ is split completely by K into linear factors.

Note, this means every polynomial of degree n which has a root in K makes K its splitting field. The converse does not hold. An irreducible polynomial of degree n does not necessarily have a splitting field of degree n . See [this answer](#).

Q9

First we prove this for an irreducible polynomial $p(x)$ with $n = \deg p(x)$ roots of the form c_1, \dots, c_n . Inductively adjoining c_1 to F forms a field $F(c_1)$ such that $[F(c_1) : F] = n$ with a basis $\{1, c_1, \dots, c_1^{n-1}\}$. Dividing $p(x)$ by $(x - c_1)$ leaves a polynomial $q(x)$ with degree $n - 1$ and adjoining the second root to $F(c_1)$ forms a field extension with degree $[F(c_1, c_2) : F(c_1)] = n - 1$. Proceeding in this way, we obtain a maximum order of $n!$.

The polynomial $a(x)$ is reducible to n irreducible factors $a(x) = p_1(x)p_2(x)\cdots p_n(x)$ where $\deg p_i(x) = k_i$. Each of these fields forms a simple extension $F(c_1, \dots, c_n)$, where $[F(c_1, \dots, c_n) : F] = [F(c_1, \dots, c_n) : F(c_1, \dots, c_{n-1})]\cdots [F(c_1) : F] = k_n \cdot k_{n-1} \cdots k_1$.

Since $\deg a(x) = N$ and $k_1 + \cdots + k_n$, so $[K : F] | k_1! \cdots k_n!$.

From the binomial formula, given $n = k + l$, then there's an integer z such that

$$z = \frac{n!}{k!l!} \implies n! = zk!!$$

So therefore given $n = k_1 + \cdots + k_n$, we can see that $x | k_1! \cdots k_n! \implies x | n!$

D. Reducing Iterated Extensions to Simple Extensions

Q1

a

$$\begin{aligned} \mathbb{Q}(\sqrt{2}, i\sqrt{3}) &= \mathbb{Q}(\sqrt{2} + i\sqrt{3}) \\ c &= \sqrt{2} + i\sqrt{3} \\ [\mathbb{Q}(c) : \mathbb{Q}] &= 4 \\ \implies \sqrt{2} &= a_0 + a_1c + a_2c^2 + a_3c^3 \\ c^2 &= 2i\sqrt{6} - 1 \implies i\sqrt{6} \in \mathbb{Q}(c) \\ c^3 &= 4i\sqrt{3} - \sqrt{2} - 6\sqrt{2} - i\sqrt{3} = 3i\sqrt{3} - 7\sqrt{2} \\ c^3 + 7c &= 10i\sqrt{3} \implies i\sqrt{3} \in \mathbb{Q}(c) \end{aligned}$$

Same can be shown for $\sqrt{2}$.

b

$$\begin{aligned} (\sqrt[6]{2})^3 &= \sqrt{2}, (\sqrt[6]{2})^2 = \sqrt[3]{2} \\ \implies \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) &= \mathbb{Q}(\sqrt[6]{2}) \end{aligned}$$

Q2

The roots of $x^2 - 2x - 1$ by completing the square are $\pm\sqrt{2} + 1$.

For a cubic with real coefficients in a field, it either has all real roots or 2 complex roots. By differentiating and sketching the curve where it's increasing or decreasing, we see that this cubic has two complex roots.

According to the **Complex Conjugate Theorem**, if $x = a + ib$ is a solution to a polynomial with real coefficients, then so is $x = a - ib$.

Thus we conclude that $\mathbb{Q}(a, b) = \mathbb{Q}(a + b)$ where a is a complex root of $x^3 - x - 1$.

Q3

These factors are all linearly independent so $c = \sqrt{2} + \sqrt{3} + \sqrt{-5}$.

Q4

From C6, because $\sqrt{2}$ and $\sqrt{3}$ are independent, the basis is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ and so the minimum polynomial has degree 4.

```
sage: # We let x = sqrt(2) + sqrt(3), so now we square it on both sides
sage: (sqrt(2) + sqrt(3))^2
(sqrt(3) + sqrt(2))^2
sage: ((sqrt(2) + sqrt(3))^2).expand()
2*sqrt(3)*sqrt(2) + 5
sage: # so now (x^2 - 5) = 2*sqrt(3)*sqrt(2)
sage: # lets square again both sides
sage: (2*sqrt(3)*sqrt(2))**2
24
sage: ((x^2 - 5)^2).expand()
x^4 - 10*x^2 + 25
sage: ((x^2 - 5)^2).expand() - 24
x^4 - 10*x^2 + 1
```

Q5

The minimum polynomial will now have degree 8.

```
sage: x - sqrt(2) == sqrt(3) + I*sqrt(5)
x - sqrt(2) == I*sqrt(5) + sqrt(3)
sage: (x - sqrt(2) == sqrt(3) + I*sqrt(5))^2
(x - sqrt(2))^2 == (I*sqrt(5) + sqrt(3))^2
sage: ((x - sqrt(2) == sqrt(3) + I*sqrt(5))^2).expand()
x^2 - 2*sqrt(2)*x + 2 == 2*I*sqrt(5)*sqrt(3) - 2
sage: ((x - sqrt(2) == sqrt(3) + I*sqrt(5))^2).expand() + 2*sqrt(2)*x
x^2 + 2 == 2*sqrt(2)*x + 2*I*sqrt(5)*sqrt(3) - 2
sage: p = ((x - sqrt(2) == sqrt(3) + I*sqrt(5))^2).expand() + 2*sqrt(2)*x
sage: p
x^2 + 2 == 2*sqrt(2)*x + 2*I*sqrt(5)*sqrt(3) - 2
sage: p += 2
sage: p
x^2 + 4 == 2*sqrt(2)*x + 2*I*sqrt(5)*sqrt(3)
sage: (p^2).expand()
x^4 + 8*x^2 + 16 == 8*I*sqrt(5)*sqrt(3)*sqrt(2)*x + 8*x^2 - 60
sage: (p^2).expand() + 60 - 8*x^2
x^4 + 76 == 8*I*sqrt(5)*sqrt(3)*sqrt(2)*x
sage: p = (p^2).expand() + 60 - 8*x^2
sage: (p^2).expand()
x^8 + 152*x^4 + 5776 == -1920*x^2
sage: (p^2).expand() + 1920*x^2
x^8 + 152*x^4 + 1920*x^2 + 5776 == 0
sage: p = x^8 + 152*x^4 + 1920*x^2 + 5776
sage: p(x = sqrt(2) + sqrt(3) + I*sqrt(5)).expand()
0
```

E. Roots of Unity and Radical Extensions

Q1

The roots of $x^n - 1$ are $1, \omega, \dots, \omega^{n-1}$ which is the basis for $\mathbb{Q}(\omega)$ generated by ω since it is primitive.

Q2

Define a substitution function σ_ω

$$\sigma_\omega(a(x)) = a(\omega)$$

σ_ω is a homomorphism because

$$\begin{aligned}\sigma_\omega(a(x)b(x)) &= a(\omega)b(\omega) \\ &= \sigma_\omega(a(x))\sigma_\omega(b(x))\end{aligned}$$

Which has a kernel of

$$\begin{aligned}\ker \sigma_\omega &= \{a(x) : \sigma_\omega(a(x)) = a(\omega) = 0\} \\ &= J\end{aligned}$$

The kernel of any homomorphism is an ideal. In $F[x]$ every ideal is a principal ideal so $J = \langle p(x) \rangle$. So $p(x)$ is a polynomial of lowest degree among all nonzero polynomials in J . Hence it is irreducible.

When n is prime, then

$$x^{n-1} + x^{n-2} + \cdots + x + 1$$

is irreducible. Therefore $p(x) = x^{n-1} + \cdots + 1$ and $p(\omega) = 0$. Since

$$\mathbb{Q}(\omega) \cong \mathbb{Q}[x]/\langle p(x) \rangle$$

Then

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg p(x) = n - 1$$

Q3

$$p(\omega) = 0 \implies \omega^{n-1} = -(\omega^{n-2} + \cdots + \omega + 1)$$

Q4

n = 6

$$x^6 - 1 = (x^3 - 1)(x^3 + 1)$$

The roots are $1, s, s^2$ and $-1, -s, -s^2$ respectively where s is the third root of unity.

But from above we know that $s^2 + s + 1 = 0 \implies s^2 = -(s + 1)$ and $s^2 \in \mathbb{Q}(s)$, so $\mathbb{Q}(\omega) = \mathbb{Q}(s)$ with basis $\{1, s\}$.

$$\begin{aligned}[\mathbb{Q}(\omega) : \mathbb{Q}] &= [\mathbb{Q}(s) : \mathbb{Q}] \\ &= 2\end{aligned}$$

n = 7

$n = 7$ is prime so $[\mathbb{Q}(\omega) : \mathbb{Q}] = 6$.

n = 8

$$\begin{aligned}x^8 - 1 &= (x^4 - 1)(x^4 + 1) \\ &= (x^2 - 1)(x^2 + 1)(x^4 + 1)\end{aligned}$$

With roots $-1, 1$ and $i, -i$ for $(x^2 - 1)$ and $(x^2 + 1)$ respectively.

The 4th roots of -1 are $\pm \frac{1}{\sqrt{2}} \pm \frac{i}{\sqrt{2}}$.

$\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{2}, i)$ with a basis $\{1, \sqrt{2}, i, \sqrt{2}i\}$ and

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$$

Q5

$$\forall r \in \{1, 2, \dots, n-1\}, (\sqrt[n]{a}\omega^r)^n = 1$$

$$|\{\sqrt[n]{a}\omega^r : r \in \{0, 1, \dots, n-1\}\}| = n$$

Q6

The basis of $\mathbb{Q}(\omega, \sqrt[n]{a})$ is the set $\{\omega^i (\sqrt[n]{a})^j\}$ where $i, j \in \{0, 1, \dots, n-1\}$, which contains the ideal for $\sigma(c) = x^n - 1$, which is $J = \{\sqrt[n]{a}, \sqrt[n]{a}\omega, \dots, \sqrt[n]{a}\omega^{n-1}\}$.

Q7

The degree of $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q}] = 2 \times 3 = 6$.

You can calculate $\cos(\pi/3)$ and $\sin(\pi/3)$ by splitting an equilateral triangle with unit sides in half. The sum of a triangle's angles will always be π , and so each corner of the equilateral triangle will be $(\pi/3)$. Use pythagoreas theorem to calculate the midline as $o^2 = 1^2 - (\frac{1}{2})^2$.

Using wolfram alpha, we see that the cube roots of 1 are $1, -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} - \frac{\sqrt{3}}{2}i$.

$$\mathbb{Q}(\omega, \sqrt[3]{2}) = \mathbb{Q}(i\sqrt{3}, \sqrt[3]{2})$$

Q8

Let s be the nth root of a in K , then it is the root of $x^n - a$. Then $\sqrt[n]{a}\omega^i$ is also a root of this polynomial. For every n there is an irreducible cyclotomic polynomial $p(x)$ with roots that consist of $\phi(n)$ nth roots of a that have a multiplicative order of n . By theorem 7, since $p(x)$ has one root in K and is irreducible, therefore all its roots are in K .

For n is not prime, $p(x) \mid x^n - a$ so all $\phi(n)$ primitive roots of $p(x)$ are also roots of $x^n - a$ and so generates all roots. We use the irreducible polynomial $p(x)$ to prove there's an isomorphism permuting roots of $p(x)$, therefore showing both fields are equivalent and contain all roots.

Fixing \mathbb{Q} , there is an isomorphism $h : \mathbb{Q}(s) \rightarrow \mathbb{Q}(\sqrt[n]{a}\omega^i)$. Note that $p(h(c)) = (h(c))^n - a = h(c^n - a) = 0$ as the function is homomorphic so $h(c)^n = h(c^n)$ and fixes \mathbb{Q} leaving a unchanged. This function is an isomorphism mapping one to one and onto, we can say that $h(x)$ permutes the roots c of $x^n - a$. So we can see that $\mathbb{Q}(s) = \mathbb{Q}(\sqrt[n]{a}\omega^i)$, and that K contains all roots of $x^n - a$.

Since the splitting field contains all powers of $\sqrt[n]{a}\omega^i$ by the isomorphism $h(x)$ as well as $\sqrt[n]{a}\omega^0 = \sqrt[n]{a}$ and also its inverse $(\sqrt[n]{a})^{-1}$ (because it's a field), so it also contains all nth roots of unity since $(\sqrt[n]{a})^{-1}(\sqrt[n]{a}\omega^i) = \omega^i$.

F. Separable and Inseparable Polynomials

Q1

From theorem 1, F has characteristic 0 \implies irreducible polynomials never have multiple roots.

Q2

Each power of x in $a(x)$ is independent, so $a_m x^m + a_n x^n \neq 0$ when $m \neq 0$ unless $a_m = a_n = 0$.

Therefore $a'(x) = \sum m_i a_i x^{m_i-1} = 0 \implies p \mid m_i$ for all m_i and all nonzero terms of $a(x)$ are of the form $a_{mp} x^{mp}$.

Q3

$$a(x) = (x - c)^2 q(x)$$
$$a'(x) = 2(x - c)q(x) + (x - c)^2 q'(x)$$

Both $a(x)$ and $a'(x)$ have c as a root, but $a(x)$ is irreducible, so $a(x) \mid a'(x)$, but this cannot be true since $\deg a'(x) < \deg a(x)$ unless $a'(x) = 0$.

From the previous answer $a'(x) = 0$ means the nonzero terms of $a(x)$ are of the form $a_{mp} x^{mp}$, and $a(x)$ is a polynomial in powers of x^p .

Q4

$a(x)$ is a polynomial in powers of $x^p \implies a'(x) = 0 \implies a(x) \mid a'(x) \implies$ share common factor of $a(x) \implies a(x)$ has a multiple root.

Q5

This follows from $[a(x) + b(x)]^p = a(x)^p + b(x)^p$ in any field of characteristic p and is proved in 24D6.

Q6

$$\begin{aligned} a(x) &= a_0 + a_1 x + \cdots + a_n x^n \\ a(x^p) &= a_0 + a_1 x^p + \cdots + a_n x^{np} \end{aligned}$$

The frobenius automorphism for a finite field of characteristic p is bijective since the function is injective, and any injective function from a finite set to itself is also surjective.

This implies the coefficients of $a(x^p)$ all have p th roots, and so

$$\begin{aligned} a(x^p) &= c_0^p + c_1^p x^p + \cdots + c_n^p x^{np} \\ &= (c_0 + c_1 x + \cdots + c_n x^n)^p \end{aligned}$$

Thus $b(x) = c_0 + c_1 x + \cdots + c_n x^n$ and $a(x^p) = [b(x)]^p$.

Q7

Assume there is an irreducible polynomial $a(x)$ that is inseparable. Then it is a polynomial in powers of x^p .

Then there is a polynomial $[b(x)]^p = a(x)$. Thus $a(x)$ is reducible, which is a contradiction.

Thus every irreducible polynomial is separable.

G. Multiple Roots over Infinite Fields of Nonzero Characteristic

Q1

There are infinite powers of y , so $\mathbb{Z}_p[y]$ is an infinite ring with characteristic p .

Thus

$$\mathbb{Z}_p(y) = \{a(y)/b(y) : a(y), b(y) \in \mathbb{Z}_p[y]\}$$

is an infinite field, and so is $\mathbb{Z}_p(y^p)$

Q2

By binomial theorem, all coefficients for the terms of $(x - y)^p$ are a factor of p . $E[x]$ has characteristic p so

$$x^p - y^p = (x - y)^p$$

However $y \notin K[x]$ so $x^p - y^p$ is irreducible in $K[x]$.

Q3

$$\bar{i}(a_0 + \cdots + a_n x^n) = i(a_0) + \cdots + i(a_n) x^n$$

but for all $a_i \in F$, $i(a_i) = a_i$ so $\bar{i}(p(x)) = p(x)$.

Q4

Expanding out $(x - a)^m$, the coefficients in F and x remain fixed, but a is mapped to b , so

$$\bar{i}((x - a)^m) = (x - b)^m$$

Q5

Since \bar{i} leaves $p(x)$ fixed, so

$$\begin{aligned} \bar{i}(p(x)) &= \bar{i}((x - a)^m s(x)) \\ &= (x - b)^m \bar{i}(s(x)) \\ &= p(x) \end{aligned}$$

so a and b have the same multiplicity in $p(x)$.

H. An Isomorphism Extension Theorem (Proof of Theorem 3)

Q1

$$F_1(a) \cong F_1[x]/\langle p(x) \rangle$$

Where $p(x)$ is the minimum polynomial with a as a root. The homomorphism $\phi : F_1[x] \rightarrow F_1(a)$ by $\phi_c(a(x)) = a(c)$ has the kernel $J = \langle p(x) \rangle$ since in $F[x]$ every ideal is a principal ideal.

Thus since $s(x) = c(x) - d(x)$ has a root a since $s(a) = 0$, so $s(x) \in J$ and it is a multiple of $p(x)$.

Observing that $h(c(x) - d(x)) = h(p(x)q(x))$, we easily see that $h(p(x)q(x)) = hp(x)hq(x)$ and also that $h(c(x) - d(x)) = hc(x) - hd(x)$ since

$$\begin{aligned} hc(x) - hd(x) &= (h(c_0) - h(d_0)) + (h(c_1) - h(d_1))x + \cdots + (h(c_n) - h(d_n))x^n \\ &= h(c_0 - d_0) + h(c_1 - d_1)x + \cdots + h(c_n - d_n)x^n \\ &= h(c(x) - d(x)) \end{aligned}$$

Q2

$$\begin{aligned} h(c(a)) &= h(c_0) + h(c_1)b + \cdots + h(c_n)b^n \\ h(d(a)) &= h(d_0) + h(d_1)b + \cdots + h(d_n)b^n \end{aligned}$$

$$\begin{aligned} h(c(a)) - h(d(a)) &= h(c_0 - d_0) + h(c_1 - d_1)b + \cdots + h(c_n - d_n)b^n \\ &= h(c(x) - d(x))(b) \\ &= [hp(x)(b)][hq(x)(b)] \end{aligned}$$

But $hp(x)(b) = 0$ so $h(c(a)) - h(d(a)) = 0 \implies h(c(a)) = h(d(a))$.

Q3

$$hc(x) = hd(x)$$

$$\begin{aligned} \implies hc(x) - hd(x) &= 0 \\ &= h(c(x) - d(x)) \\ &= h(c_0 - d_0) + h(c_1 - d_1)x + \cdots + h(c_n - d_n)x^n \end{aligned}$$

But h is isomorphic on $F_1 \rightarrow F_2$ so $c_i = d_i \implies c(x) = d(x)$.

Q4

$h(a) = b$, there is no other value that produces b .

All the coefficients for a polynomial $c(x)$ are reversible.

$$c(x) = h^{-1}(h(c_0)) + h^{-1}(h(c_1))x + \cdots + h^{-1}(h(c_n))x^n$$

Q5

$$\begin{aligned} h(c(x) + d(x)) &= h(c_0 + d_0) + h(c_1 + d_1)x + \cdots + h(c_n + d_n)x^n \\ &= (h(c_0) + h(d_0)) + (h(c_1) + h(d_1))x + \cdots + (h(c_n) + h(d_n))x^n \\ &= hc(x) + hd(x) \end{aligned}$$

$$\begin{aligned} h(c(x)d(x)) &= h(c_0d_0) + h(\sum_{i+j=1} c_id_jx) + h(\sum_{i+j=2} c_id_jx^2) + \cdots + h(\sum_{i+j=n} c_id_jx^n) \\ &= h(c_0)h(d_0) + \sum_{i+j=1} h(c_i)h(d_j)x + \sum_{i+j=2} h(c_i)h(d_j)x^2 + \cdots + \sum_{i+j=n} h(c_i)h(d_j)x^n \\ &= hc(x)hd(x) \end{aligned}$$

I. Uniqueness of the Root Field

Q1

First note that

$$F_1(u) \cong F_1[x]/\langle p(x) \rangle$$

Let $f : F_1[x] \rightarrow F_2(v)$ defined by

$$f(a(x)) = h(a(x))(v)$$

Then the ideal is $J = \langle p(x) \rangle$

$$\begin{aligned} f(a(x)) = f(b(x)) &\iff f(a(x)) - f(b(x)) = 0 \\ &\iff f(a(x) - b(x)) = 0 \\ &\iff a(x) - b(x) \in J \\ &\iff J + a(x) = J + b(x) \end{aligned}$$

Let $\phi : F_1[x]/\langle p(x) \rangle \rightarrow F_2(v)$ by

$$\phi(J + a(x)) = f(a(x)) = h(a(x))(v)$$

We can see that this function is an isomorphism:

- **injective:** $\phi(J + a(x)) = \phi(J + b(x)) \implies f(a(x)) = f(b(x))$
 $\implies J + a(x) = J + b(x)$

- **surjective:** $h(a(x))(v) = h(a(u))$ which is **onto** $F_2(v)$ and surjective, so $f(a(x)) = \phi(J + a(x))$ is surjective.
- Finally,

$$\begin{aligned} \phi(J + a(x)) + \phi(J + b(x)) &= f(a(x)) + f(b(x)) \\ &= [ha(x) + hb(x)](v) \\ &= h(a(x) + b(x))(v) \\ &= \phi(J + a(x) + b(x)) \\ \\ \implies F_2(v) &\cong F_1[x]/\langle p(x) \rangle \\ F_1(u) &\cong F_1[x]/\langle p(x) \rangle \\ F_1(u) &\cong F_2(v) \end{aligned}$$

Q2

We start with $F_1(u) = K_1$ and want to prove that this means $F_2(v) = K_2$. This will also automatically prove the converse statement if shown to be true.

Let $p(x)$ be the minimum polynomial $p(x)$ for u such that $p(u) = 0$.

$h : F_1(u) \rightarrow F_2(v)$ but $F_1(u) = K_1$ so $h : K_1 \rightarrow F_2(v)$, but h is surjective and so $\deg p(x) = \deg hp(x)$ since both $p(x)$ and $hp(x)$ are irreducible.

$$\begin{aligned} \forall u_i \in K_1 : p(u_i) = 0, \exists v_i = h(u_i) : hp(v_i) = 0 \\ \implies F_2(v) = K_2 \end{aligned}$$

Because there are $\deg hp(x) = \deg p(x)$ such roots v_i which correspond to u_i roots of $p(x)$.

Q3

$$\begin{aligned} a(x) &= p(x)q(x) \\ p(u) &= 0 \end{aligned}$$

$$\begin{aligned} h(p(u)) &= h(p(x))(v) = 0 \\ &= [hp(x)](v) = hp(v) \end{aligned}$$

Since both are equivalent.

We see that v is a root of $hp(x)$.

$$F_1(u) = K_1$$

If $F_1(u) = K_1$, then $F_1(u)$ contains all roots of $p(x)$ and then

$$F_1(u) = K_1 \iff F_2(v) = K_2$$

Recalling that $p(x)$ is an irreducible factor of $a(x)$,

$$\begin{aligned} u &\in K_1 \\ p(u) &= 0 \\ v &\in K_2 \\ hp(v) &= 0 \\ \implies F_1(u) &\cong F_2(v) \end{aligned}$$

Putting both together

$$K_1 \cong K_2$$

$$F_1(u) \neq K_1$$

See that we can extend h fixing the base field.

$$\begin{aligned} h(u) &= v \\ h : F_1(u) &\rightarrow F_2(v) \end{aligned}$$

In $F_1(u)[x]$, $a(x) = (x - u)a_1(x)$.

In $F_2(v)[x]$, $ha(x) = (x - v)ha_1(x)$.

And $\deg a_1(x) = \deg ha_1(x) = n - 1$

Now let there be a new $u' \in K_1$, $u' \notin F_1(u')$, $p(u') = 0$ and likewise for $hp(x)$ and v .

$$\deg a(x) = 1$$

Lastly when $n = \deg a(x) = 1$, then $K_1 = F_1$ and $K_2 = F_2$, since the basis are simply scalars and $a(x)$ is of the form $(x - a)$. The root of $a(x)$ is in F_1 itself, and h is an isomorphism from $F_1 \rightarrow F_2$ so

$$K_1 \cong K_2$$

Q4

$$u \in K_1, v \in K_2$$

But $F_1 = F_2$

$$\begin{aligned} h : F[x] &\rightarrow F[x] \\ \forall a \in F, h(a) &= a \\ h &= \text{id}_F \\ h(u) &= v \\ \implies K_1 &\cong K_2 \end{aligned}$$

J. Extending Isomorphism

Q1

$$h : \mathbb{Q}(\omega) \rightarrow \mathbb{C}, \forall a \in \mathbb{Q}, h(a) = a$$

Let $b \in \mathbb{Q}(\omega)$

$$\begin{aligned} b &= s_0 + s_1\omega + s_2\omega^2 + \dots + s_{p-1}\omega^{p-1} \\ h(b) &= s_0 + s_1h(\omega) + s_2h(\omega)^2 + \dots + s_{p-1}\omega^{p-1} \end{aligned}$$

So h is determined by $h(\omega)$.

Since isomorphisms preserve roots, we deduce they permute roots. There are $p - 1$ roots for the minimum polynomial of ω which has degree $p - 1$.

Q2

$p(x)$ is irreducible in $F[x]$. $c \in \mathbb{C} : p(c) = 0$.

Let $h : F \rightarrow \mathbb{C}$ be a monomorphism (injective homomorphism), then $h : F \rightarrow h(F)$ is an isomorphism and

$$F \cong h(F)$$

The minimum polynomial are $p(x)$ and $hp(x)$ respectively with $\deg p(x) = \deg hp(x) = n$. Since h permutes roots and by theorem 7 contains all roots, there are n possible monomorphisms.

Q3

$$h : F \rightarrow h(F)$$

$$\phi : K \rightarrow \mathbb{C}$$

$$[K : F] = n$$

So K forms a splitting field over F for a minimum polynomial $p(x) \in F[x]$ of degree n .

From the previous question we see that there are n monomorphisms $F(c) = K \rightarrow \mathbb{C}$.

Q4

$$h : \mathbb{Q} \rightarrow \mathbb{C}$$

$$h(x) = x$$

$$h(x) = h(y) \implies x = y$$

$$h(1) = 1_{\mathbb{C}}$$

$$\begin{aligned} h\left(\frac{n}{n}\right) &= h\left(\frac{1}{n} + \cdots + \frac{1}{n}\right) \\ 1 &= nh\left(\frac{1}{n}\right) \\ \implies h\left(\frac{1}{n}\right) &= \frac{1}{n} \end{aligned}$$

$$\begin{aligned} h\left(\frac{p}{q}\right) &= h\left(\frac{1}{q} + \cdots + \frac{1}{q}\right) \\ &= \underbrace{h\left(\frac{1}{q}\right) + \cdots + h\left(\frac{1}{q}\right)}_p \\ &= \frac{p}{q} \end{aligned}$$

Thus all monomorphisms $h : \mathbb{Q}(a) \rightarrow \mathbb{C}$ fix \mathbb{Q} .

Q5

$$\mathbb{Q}(\sqrt[3]{2}) \rightarrow \mathbb{C}$$

Minimum polynomial for $c = \sqrt[3]{2}$ is $p(x) = x^3 - 2$

Three roots of $p(x)$ are $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$.

\mathbb{Q} remains fixed. Roots are permuted (see above questions).

Three monomorphisms are

$$\sqrt[3]{2} \rightarrow \sqrt[3]{2}$$

$$\sqrt[3]{2} \rightarrow \sqrt[3]{2}\omega$$

$$\sqrt[3]{2} \rightarrow \sqrt[3]{2}\omega^2$$

K. Normal Extensions

Q1

K is a finite extension of $F \implies K$ is a simple extension and so that $K = F(c)$.

There is a minimum polynomial $p(x)$ for c in F .

So by the question K is a normal extension.

Q2

K is a finite extension of $F \implies K = F(c)$.

Let $p(x)$ be the minimum polynomial for c , so $p(c) = 0$.

Let h be an isomorphism fixing F

$$h : K \rightarrow h(K)$$

Then by the question $h(K) \subseteq K$ and since h is an isomorphism where $K \cong h(K)$, so $h(K) = K$, and $h : K \rightarrow K$ is an automorphism fixing F and permuting roots of $p(x)$.