Abstract Algebra by Pinter, Chapter 32

Amir Taaki

Chapter 32 on Galois Theory Preamble

Contents

A. Computing a Galois Group

Q1

All the roots of $(x^2+1)(x^2-2)$ are $\pm i, \pm\sqrt{2} \in \mathbb{Q}(i, \sqrt{2})$.

Q2

$$\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i)(\sqrt{2})$$

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

$$[\mathbb{Q}(i) : \mathbb{Q}] = 2$$

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

Since $\sqrt{2} \notin \mathbb{Q}(i)$ and it's minimum polynomial is (x^2-2).

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

Q3

Permutations are:

$$\{\{i, \sqrt{2}\}, \{-i, \sqrt{2}\}, \{i, -\sqrt{2}\}, \{-i, -\sqrt{2}\}\}$$

$$k_0 + k_1 i + k_2\sqrt{2} + k_3 i\sqrt{2}) \xrightarrow{\quad e \quad} k_0 + k_1 i + k_2\sqrt{2} + k_3 i\sqrt{2}$$
$$k_0 + k_1 i + k_2\sqrt{2} + k_3 i\sqrt{2}) \xrightarrow{\quad a \quad} k_0 - k_1 i + k_2\sqrt{2} - k_3 i\sqrt{2}$$
$$k_0 + k_1 i + k_2\sqrt{2} + k_3 i\sqrt{2}) \xrightarrow{\quad b \quad} k_0 + k_1 i - k_2\sqrt{2} - k_3 i\sqrt{2}$$
$$k_0 + k_1 i + k_2\sqrt{2} + k_3 i\sqrt{2}) \xrightarrow{\quad c \quad} k_0 - k_1 i - k_2\sqrt{2} + k_3 i\sqrt{2}$$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$$\mathrm{Gal}(\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}) = \{e, a, b, c\}$$

Q4

Base field is $\mathbb{Q}$ which corresponds to e.

b maps $\{i, \sqrt{2} \to i, -\sqrt{2}\}$ and so leaves i fixed. It corresponds to $\mathbb{Q}(i)$. Likewise a leaves $\sqrt{2}$ fixed and corresponds to $\mathbb{Q}(\sqrt{2})$. The last one c corresponds to $\mathbb{Q}(i\sqrt{2})$.

B. Computing a Galois Group of Eight Elements

Q1

$(x^2 - 2)$ is irreducible over $\mathbb{Q}$ because if $(x^2 - 2) = (x + a)(x + b)$ where $a, b \in \mathbb{Z}$, then

$$a + b = 0, ab = -2 \implies a = -b, a^2 = 2$$

So $a^2 = 2$ which is impossible. Likewise for $(x^2 - 3)$ and $(x^2 - 5)$ which form extension fields over $\mathbb{Q}$.

$$\mathbb{Q}(\sqrt{2})(\sqrt{3})(\sqrt{5}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$$

Q2

The degree of the field extension is 8 since the minimum polynomial is degree 8.

Q3

$$\alpha : \begin{cases} \sqrt{2} & \mapsto -\sqrt{2} \\ \sqrt{3} & \mapsto \sqrt{3} \\ \sqrt{5} & \mapsto \sqrt{5} \end{cases} \qquad \beta : \begin{cases} \sqrt{2} & \mapsto \sqrt{2} \\ \sqrt{3} & \mapsto -\sqrt{3} \\ \sqrt{5} & \mapsto \sqrt{5} \end{cases} \qquad \gamma : \begin{cases} \sqrt{2} & \mapsto \sqrt{2} \\ \sqrt{3} & \mapsto \sqrt{3} \\ \sqrt{5} & \mapsto -\sqrt{5} \end{cases}$$

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}) = \{1, \alpha, \beta, \gamma, \alpha\beta, \alpha\gamma, \beta\gamma, \alpha\beta\gamma\}$$

Table can be constructed by noting the group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

	e	a	b	c	ab	ac	bc	abc
e	e	a	b	c	ab	ac	bc	abc
a	a	e	ab	ac	b	c	abc	bc
b	b	ab	e	bc	a	abc	c	ac
c	c	ac	bc	e	abc	a	b	ab
ab	ab	b	a	abc	e	bc	ac	c
ac	ac	c	abc	a	bc	e	ab	b
bc	bc	abc	c	b	ac	ab	e	a
abc	abc	bc	ac	ab	c	b	a	e

Q4

We know the group is of order 8, so there are subgroups of order 1, 2, 4, and 8.

The order 1 subgroup is the trivial $1 = \{e\}$ which fixes $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, and the subgroup of order 8 is simply $\mathbf{G}$.

Order 2

These are the groups $\langle\alpha\rangle, \langle\beta\rangle, \langle\gamma\rangle, \langle\alpha\beta\rangle, \langle\alpha\gamma\rangle, \langle\beta\gamma\rangle, \langle\alpha\beta\gamma\rangle$.

Order 4

These are groups of the form $\langle x, y\rangle = \{1, x, y, xy\}$ where x and y are any distinct elements from $\alpha, \beta, \gamma, \alpha\beta, \alpha\gamma, \beta\gamma, \alpha\beta\gamma$. Note that $\langle x, xy\rangle = \langle x, y\rangle$.

Q5

First note the Galois correspondences where $H \subseteq \mathbf{G}$ is a subgroup, and K_H is the fixfield for $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

$$H \mapsto K_H = \{a \in \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \pi(a) = a \text{ for every } \pi \in H\}$$

$$K_H \mapsto \mathrm{Aut}(K_H) = H = \{\pi \in \mathbf{G} : \pi(a) = a \text{ for every } a \in K_H\}$$

$$\begin{aligned}
H &= \{e\} && \mapsto K_H = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \\
H &= \mathbf{G} && \mapsto K_H = \mathbb{Q} \\
H &= \langle\alpha\rangle && \mapsto K_H = \mathbb{Q}(\sqrt{3}, \sqrt{5}) \\
H &= \langle\beta\rangle && \mapsto K_H = \mathbb{Q}(\sqrt{2}, \sqrt{5}) \\
H &= \langle\gamma\rangle && \mapsto K_H = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\
H &= \langle\alpha\beta\rangle && \mapsto K_H = \mathbb{Q}(\sqrt{5}, \sqrt{6}) \\
H &= \langle\alpha\gamma\rangle && \mapsto K_H = \mathbb{Q}(\sqrt{3}, \sqrt{10}) \\
H &= \langle\beta\gamma\rangle && \mapsto K_H = \mathbb{Q}(\sqrt{2}, \sqrt{15}) \\
H &= \langle\alpha\beta\gamma\rangle && \mapsto K_H = \mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) = \mathbb{Q}(\sqrt{6}, \sqrt{10}) \\
H &= \langle\alpha, \beta\rangle && \mapsto K_H = \mathbb{Q}(\sqrt{5}) \\
H &= \langle\alpha, \gamma\rangle && \mapsto K_H = \mathbb{Q}(\sqrt{3}) \\
H &= \langle\beta, \gamma\rangle && \mapsto K_H = \mathbb{Q}(\sqrt{2}) \\
H &= \langle\alpha, \beta\gamma\rangle && \mapsto K_H = \mathbb{Q}(\sqrt{15}) \\
H &= \langle\beta, \alpha\gamma\rangle && \mapsto K_H = \mathbb{Q}(\sqrt{10}) \\
H &= \langle\gamma, \alpha\beta\rangle && \mapsto K_H = \mathbb{Q}(\sqrt{6}) \\
H &= \langle\alpha\beta, \beta\gamma\rangle = \{1, \alpha\beta, \beta\gamma, \alpha\gamma\} && \mapsto K_H = \mathbb{Q}(\sqrt{30}) \\
&= \langle\alpha\gamma, \beta\gamma\rangle
\end{aligned}$$

C. A Galois Group Equal to S_3

Q1

From 31E6 we proved that $\mathbb{Q}(\omega, \sqrt[n]{a})$ is the splitting field of $x^n - a$ over $\mathbb{Q}$.

The primitive cube root of unity is $\omega = \frac{-1+i\sqrt{3}}{2} \in \mathbb{Q}(i\sqrt{3})$.

Thus $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2})$ is the splitting field of $x^3 - 2$.

Q2

Since $x^3 - 2$ is irreducible over $\mathbb{Q}$, and contains $\sqrt[3]{2}$, the field $\mathbb{Q}(\sqrt[3]{2}) = \{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2$ has degree 3.

Q3

x^2+3 has roots $i\sqrt{3}, -i\sqrt{3} \notin \mathbb{Q}(\sqrt[3]{2})$ and so is irreducible. Thus $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}(\sqrt[3]{2})] = 2$.

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

Q4

Since there is a congruence relation between a galois field and it's fixfield, we can conclude that $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q})$ has 6 elements.

Every automorphism of K fixing F is completely determined by a permutation of the roots of $a(x)$.

Thus every element of **G** is determined by a permutation of the 3 cube roots of 2.

Q5

The group S_3 is defined as a permutation of 3 elements and consists of the 6 elements:

$$\begin{array}{ccc} \epsilon = (1)(2)(3) & \beta = (23) & \gamma = (132) \\ \gamma = (12) & \delta = (123) & \kappa = (13) \end{array}$$

Which is precisely the structure of $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q})$.

D. A Galois Group Equal to D_4

Q1

The 4 roots of x^4-2 are $\pm\alpha, \pm i\alpha$. Thus $\mathbb{Q}(\pm\alpha, \pm i\alpha) = \mathbb{Q}(\alpha, i)$ is the splitting field for x^4-2.

Q2

The minimum polynomial for $\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3\}$ is of degree 4, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

Q3

$\mathbb{Q}(\alpha)$ is a subfield of $\mathbb{R}$ so $i \notin \mathbb{Q}(\alpha)$. The minimum polynomial for i over $\mathbb{Q}(\alpha)$ is x^2+1 which is degree 2. So $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$.

Q4

$$[\mathbb{Q}(\alpha, i) : \mathbb{Q}] = [\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \times 4 = 8$$

Q5

The basis for $\mathbb{Q}(\alpha, i)/\mathbb{Q}(\alpha)$ is $\{1, i\}$ since the field is of degree 2. The basis for $\mathbb{Q}(\alpha)/\mathbb{Q}$ is degree 4 and $\{1, \alpha, \alpha^2, \alpha^3\}$. Thus the basis for $\mathbb{Q}(\alpha, i)/\mathbb{Q}$ is $\{1, \alpha, \alpha^2, \alpha^3, i\alpha, i\alpha^2, i\alpha^3\}$.

Q6

$\mathbb{Q}$ remains fixed in the automorphism. Since the elements in the basis are independent, h is determined by its effect on elements in the basis.

Since any element consists of a linear sum of basis elements, which themselves consist of factors of α and i, then h is determined by its effect on $h(\alpha)$ and $h(i)$.

Let $c \in \mathbb{Q}(\alpha, i)$, then

$$\begin{aligned} h(c) &= h(c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 + c_4 i + c_5 i\alpha^2 + c_6\alpha^3) \\ &= c_0 + c_1 h(\alpha) + c_2 h(\alpha)^2 + c_3 h(\alpha)^3 + c_4 h(i) + c_5 h(i)h(\alpha)^2 + c_6 h(i)h(\alpha)^3 \end{aligned}$$

Q7

We know that $\alpha^4 - 2 = 0$, so $h(\alpha^4 - 2) = h(\alpha)^4 - 2 = 0 \implies h(\alpha)$ is a fourth root of 2 $\implies h(\alpha) \in \{\alpha, -\alpha, i\alpha, -i\alpha\}$. Likewise $i^2 + 1 = 0$, so $h(i^2 + 1) = h(i)^2 + 1 = 0 \implies h(i) = \pm i$.

$$e : \begin{cases} \alpha & \mapsto \alpha \\ i & \mapsto i \end{cases} \quad a : \begin{cases} \alpha & \mapsto -\alpha \\ i & \mapsto i \end{cases} \quad b : \begin{cases} \alpha & \mapsto \alpha \\ i & \mapsto -i \end{cases} \quad c : \begin{cases} \alpha & \mapsto -\alpha \\ i & \mapsto -i \end{cases}$$

$$d : \begin{cases} \alpha & \mapsto i\alpha \\ i & \mapsto i \end{cases} \quad f : \begin{cases} \alpha & \mapsto -i\alpha \\ i & \mapsto i \end{cases} \quad g : \begin{cases} \alpha & \mapsto i\alpha \\ i & \mapsto -i \end{cases} \quad h : \begin{cases} \alpha & \mapsto -i\alpha \\ i & \mapsto -i \end{cases}$$

Q8

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

Note that $D_4 = \{R_0, R_1, R_2, R_3, R_4, R_4 \circ R_1, R_4 \circ R_2, R_4 \circ R_3\}$ which matches our group structure. Hence they are isomorphic.

E. A Cyclic Galois Group

Q1

Roots of $x^7 - 1$ are $1, \omega, \omega^2, \dots, \omega^6$, where ω is the primitive 7th root of unity. See that $1 + \omega + \dots + \omega^6 = 0$ since $n = 7$ is prime. Then $\omega^6 = -(1 + \omega + \dots + \omega^5)$ and so is a linear combo of the other ω powers. Hence $[K : \mathbb{Q}] = 6$.

Q2

Every $h \in \mathrm{Gal}(K : \mathbb{Q})$ fixes $\mathbb{Q}$, and since h is a homomorphism for a minimum polynomial $a(x)$, we observe that

$$h(a(c)) = a_0 + a_1 h(c) + \dots + a_n h(c)^n$$

When c is a root of $a(x)$, then $h(a(c)) = a(h(c)) = 0$ and hence $h(c)$ is also a root of $a(x)$. Since $1+\omega+\dots+\omega^6 = 0$, so all the 7th roots of unity are roots of this polynomial. Hence any automorphism in $\mathbf{G}$ must send $h(\alpha)$ to another 7th root of unity. Since all the roots of unity are powers of $\alpha = \omega$, and h is homomorphic such that $h(\omega^k) = h(\omega)^k$, so we can define all permutations of ω^k simply in terms of $h(\omega)$.

Also note the basis for $K/\mathbb{Q}$ is $\{1, \omega, \dots, \omega^5\}$. Hence the automorphism of the field is completely defined by $h(\alpha)$.

Q3

$$e : \{\alpha \mapsto \alpha\}, \qquad a : \{\alpha \mapsto \alpha^2\}, \qquad b : \{\alpha \mapsto \alpha^3\}$$
$$c : \{\alpha \mapsto \alpha^4\}, \qquad d : \{\alpha \mapsto \alpha^5\}, \qquad f : \{\alpha \mapsto \alpha^6\}$$

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	c	f	e	b	d
b	b	f	a	d	e	c
c	c	e	d	a	f	b
d	d	b	e	f	c	a
f	f	d	c	b	a	e

Observing the group structure we see it is isomorphic to $\mathbb{Z}_7^\times$ which itself is isomorphic to $\mathbb{Z}_6$.

Q4

Subgroups are $\{e, a, c\}, \{e, b, d\}, \{e, f\}$

Q5

See 31E4, where we find the basis for L is $\{1, \omega\}$. Thus there are no subfields between $\mathbb{Q}$ and L.

Q6

$\alpha = \sqrt[6]{2}$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. $x^2 + 3$ is irreducible because there are no complex roots in $\mathbb{Q}(\alpha)$. Hence $[\mathbb{Q}(\alpha, \sqrt{3}i) : \mathbb{Q}(\alpha)] = 2$.

$$\omega = \frac{1}{2} + \frac{\sqrt{3}}{2}i$$

The complex 6th roots of unity are $\alpha, \alpha\omega, \alpha\omega^2, \alpha\omega^3, \alpha\omega^4, \alpha\omega^5$.

$$[\mathbb{Q}(\alpha, i\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\alpha, isqrt3) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 12$$

So any automorphism defined over $\mathbb{Q}(\alpha, \sqrt{3}i)$ must send 6th roots of 2 to each other, and $\sqrt{3}i \mapsto \pm\sqrt{3}i$.

$$e : \begin{cases} \alpha & \mapsto \alpha \\ i\sqrt{3} & \mapsto i\sqrt{3} \end{cases} \quad a : \begin{cases} \alpha & \mapsto \alpha\omega \\ i\sqrt{3} & \mapsto i\sqrt{3} \end{cases} \quad b : \begin{cases} \alpha & \mapsto \alpha\omega^2 \\ i\sqrt{3} & \mapsto i\sqrt{3} \end{cases} \quad c : \begin{cases} \alpha & \mapsto \alpha\omega^3 \\ i\sqrt{3} & \mapsto i\sqrt{3} \end{cases}$$

$$d : \begin{cases} \alpha & \mapsto \alpha\omega^4 \\ i\sqrt{3} & \mapsto i\sqrt{3} \end{cases} \quad f : \begin{cases} \alpha & \mapsto \alpha\omega^5 \\ i\sqrt{3} & \mapsto i\sqrt{3} \end{cases} \quad g : \begin{cases} \alpha & \mapsto \alpha \\ i\sqrt{3} & \mapsto -i\sqrt{3} \end{cases} \quad h : \begin{cases} \alpha & \mapsto \alpha\omega \\ i\sqrt{3} & \mapsto -i\sqrt{3} \end{cases}$$

$$j : \begin{cases} \alpha & \mapsto \alpha\omega^2 \\ i\sqrt{3} & \mapsto -i\sqrt{3} \end{cases} \quad k : \begin{cases} \alpha & \mapsto \alpha\omega^3 \\ i\sqrt{3} & \mapsto -i\sqrt{3} \end{cases} \quad l : \begin{cases} \alpha & \mapsto \alpha\omega^4 \\ i\sqrt{3} & \mapsto -i\sqrt{3} \end{cases} \quad m : \begin{cases} \alpha & \mapsto \alpha\omega^5 \\ i\sqrt{3} & \mapsto -i\sqrt{3} \end{cases}$$

Let $\phi = a = \left\{\begin{cases} \alpha & \mapsto \alpha\omega \\ i\sqrt{3} & \mapsto i\sqrt{3} \end{cases}\right\}$ then $b = \phi^2, c = \phi^3, d = \phi^4, f = \phi^5$. Let $\psi = \left\{\begin{cases} \alpha & \mapsto \alpha \\ i\sqrt{3} & \mapsto -i\sqrt{3} \end{cases}\right\}$ then $h = \psi\phi, j = \psi\phi^2, k = \psi\phi^3, l = \psi\phi^4, m = \psi\phi^5$.

$$\mathbf{G} = \{e, \phi, \phi^2, \phi^3, \phi^4, \phi^5, \psi, \psi\phi, \psi\phi^2, \psi\phi^3, \psi\phi^4, \psi\phi^5\}$$

From Wikipedia, there are only two abelian groups of order 12. Namely

$$\mathbb{Z}_3 \times \mathbb{Z}_4 \qquad D_6 \cong \mathbb{Z}_6 \times \mathbb{Z}_4$$

As we can see the group is a product of two subgroups, and so is isomorphic to D_6.

F. A Galois Group Isomorphic to S_5

Q1

By Eisenstein's criteria, 2 divides all coefficients except a_n, and $2^2 \nmid a_0 = 2$.

Q2

```
sage: a = x^5 - 4*x^4 + 2*x + 2
sage: diff(a, x)
5*x^4 - 16*x^3 + 2
sage: plot(a, xmin=-5, xmax=5, ymin=-5, ymax=5)
Launched png viewer for Graphics object consisting of 1 graphics primitive
```

Q3

```
sage: x = polygen(QQ, "x")
sage: N.<a> = NumberField(x^5 - 4*x^4 + 2*x + 2)
sage: N
Number Field in a with defining polynomial x^5 - 4*x^4 + 2*x + 2
sage: x^5 - 4*x^4 + 2*x + 2
x^5 - 4*x^4 + 2*x + 2
sage: type(x^5 - 4*x^4 + 2*x + 2)
<class 'sage.rings.polynomial.polynomial_rational_flint.Polynomial_rational_flint'>
sage: # a is a root of the polynomial
sage: p = x^5 - 4*x^4 + 2*x + 2
sage: p(a)
0
sage: N.degree()
5
```

$p(x)$ is a minimum polynomial, and since $J = \langle p(x) \rangle$, so adjoining the root r_1 to $\mathbb{Q}$ forms a degree 5 extension. Since $\mathbb{Q}(r_1)$ is a subfield of K, and $K = \mathbb{Q}(r_1, \dots, r_5)$ then

$$[K : \mathbb{Q}] = [\mathbb{Q}(r_1, \dots, r_5) : \mathbb{Q}(r_1, \dots, r_4)] \cdots [\mathbb{Q}(r_1) : \mathbb{Q}] \implies [K : \mathbb{Q}] \mid [\mathbb{Q}(r_1) : \mathbb{Q}]$$

Q4

Cauchy's theorem states that any prime factor of the group order must mean the group posesses an element of that prime order.

$[K : \mathbb{Q}] \mid 5$, and there is a bijection between K (the splitting field of the minimum polynomial) and its galois group $\implies |\mathrm{Gal}(K : \mathbb{Q})|$ divides 5 $\implies$ there is an order 5 element in the group.

Since the homomorphism on the roots permutes $\{r_1, \dots, r_5\}$ and we know the Galois field has an element a of order 5, thus the cycle cannot be disjoint.

Q5

Since the polynomial has real coefficients, for every complex root, there also must be its conjugate. See the complex conjugate root theorem.

There are 2 complex roots of the form $a + ib$ and $a - ib$ with the minimum polynomial $x^2 - (a^2 - b^2)$, that forms a degree 2 extension over $\mathbb{Q}$. Any automorphism must preserve this structure.

Q6

The pair of cycles (12) and $(12 \cdots n)$ generates S_n when n is prime. See 8H5.

The inverse $(12 \cdots n)^{-1}$ is simply $(12 \cdots n)^{n-1}$.

With $(12 \cdots n)(12)(12 \cdots n)^{-1} = (23)$, and $(12 \cdots)(23)(12 \cdots n)^{-1} = (34)$ and so on. Combining these we can create all possible permutations. Thus we generate the group S_5.

Thus $\mathrm{Gal}(K : \mathbb{Q}) = S_5$.

G. Shorter Questions Relating to Automorphisms and Galois Groups

Q1

$$F(a) = \{k_0 + k_1 a + \cdots + k_n a^n : k_i \in F\} \text{ where } n = \mathrm{ord}(a)$$

Q2

$$F(a)^* = \{\pi \in \mathrm{Gal}(K : F) : \pi(a) = a \text{ for every } a \in F(a)\}$$
$$F(b)^* = \{\pi \in \mathrm{Gal}(K : F) : \pi(a) = a \text{ for every } a \in F(b)\}$$

$$
\begin{aligned}
F(a)^* \cap F(b)^* &= \{\pi \in \mathrm{Gal}(K:F) : \pi(a) = a \text{ for every } a \in F(a) \text{ and } F(b)\} \\
&= \{\pi \in \mathrm{Gal}(K:F) : \pi(a) = a \text{ for every } a \in F(a,b)\} \\
&= F(a,b)^*
\end{aligned}
$$

Q3

The minimum polynomial $p(x) = x^2 - 2$ has 2 other complex roots which do not lie in $\mathbb{R}$. Thus any automorphism mapping from $\mathbb{R} \to \mathbb{R}$ will leave $c = \sqrt[3]{2}$ untouched, and so the only automorphism for this field fixing $\mathbb{Q}$ is the identity function.

Q4

Theorem 1 states that any field extension can be represented as a simple field extension $F(c)$, and that any automorphism will map to other roots in that field extension (of which there are n possibilities for degree n minimum polynomial). However the field extension $F(c)$ does not contain all roots of $p(x)$ so the theorem is not applicable here.

Q5

Since $\mathbb{Q}(\omega)$ contains all roots for $p(x) = x^p - 1$, then h must map roots of $p(x)$ to each other while fixing $\mathbb{Q}$. The roots are generated by the primitive root of unity ω, so $h(\omega) = \omega^k$ for some k such that $1 \leq k \leq p-1$.

Q6

Let $g, h \in \mathrm{Gal}(\mathbb{Q}(\omega), \mathbb{Q})$, then $g \circ h = h \circ g = \omega^{j+k}$.

Q7

We know that $\omega^p = 1$, so all automorphisms apart from the identity function will generate the entire group through composition, because $gcd(k,p) = 1 \quad \forall k : 2 \leq k \leq p-1$. k operates in the group $\mathbb{Z}_p$ which is cyclic.

H. The Group of Automorphisms of $\mathbb{C}$

Q1

$h(1) = 1$ and $h(2) = h(1+1) = h(1) + h(1) = 2$, and so $h(a) = a$ for all $a \in \mathbb{Z}$. Applying the same logic with the other operations, we can reason that $\mathbb{Q}$ remains fixed.

Q2

$h : \mathbb{R} \to \mathbb{R}$ then $h(a) = h(\sqrt{a})h(\sqrt{a})$, and every positive number has a root in $\mathbb{R}$, so all automorphisms of $\mathbb{R}$ send positive numbers to positive numbers.

Q3

$$a < b \implies 0 < b - a \implies 0 < h(b-a) \implies h(a) < h(b)$$

Q4

Let $a < r < h(a)$ where $r \in \mathbb{Q}$. So then $h(r) = r$ yielding the identities

$$h(r) < h(a) \qquad a < r$$

Which is a contradiction. So $h(a) = a$ for all $a \in \mathbb{R}$.

Q5

$$e(a + ib) = a + ib, \qquad h(a + ib) = a - ib$$

Q6

Both functions fix $\mathbb{R}$ and are the only automorphisms in $\mathrm{Gal}(\mathbb{C} : \mathbb{R})$.

I. Further Questions Relating to Galois Groups

Q1

Composition of automorphisms of K which fix I will only ever produce automorphisms which fix I and so are in I^*. Thus I^* is a subgroup of $\mathbf{G}$.

Q2

Every fixfield of any subgroup in $\mathbf{G}$ will contain F since all automorphisms in $\mathbf{G}$ fix F.

Let $a, b \in H^\circ$, then $\pi(ab) = \pi(a)\pi(b) = ab$, $\pi(a+b) = a+b$ for every $\pi \in H$. Lastly $\pi(aa^{-1}) = aa^{-1}$ so H° contains inverses. So H° is a subfield of K.

Q3

H is the fixer of I so

$$H = \text{Gal}(I : F)$$

I' is the fixfield of H so

$$I' = \{a \in K : \pi(a) = a \quad \forall \pi \in H\}$$

By definition, all elements of H fix I and $I \subseteq K$, so therefore $I \subseteq I'$.

I is the fixfield of H

$$I = \{a \in K : \pi(a) = a \quad \forall \pi \in H\}$$

and I^* the fixer of I

$$I^* = \text{Gal}(I : F)$$

Let $g \in H$, then for all $a \in I, g(a) = a \implies g \in \text{Gal}(I : F) = I^* \implies H \subseteq I^*$.

Q4

$$\text{Gal}(I : F) \cong \frac{\text{Gal}(K : F)}{\text{Gal}(K : I)}$$
$$\mathbf{G} = \text{Gal}(K : F)$$

Every subgroup of an abelian group is abelian. Every homomorphic image is also abelian.

$\text{Gal}(K : I)$ is a normal subgroup of $\mathbf{G}$, and $\text{Gal}(I : F)$ is the homomorphic image of $\text{Gal}(K : F)$ with $\ker \phi = \text{Gal}(K : I)$.

Q5

- Subgroups of cyclic groups are cyclic
- Homomorphic image of a cyclic group is cyclic

By the above logic we conclude the Galois groups are cyclic.

Q6

Every cyclic group is the direct product of cyclic groups. From the fundamental theorem of cyclic groups for a finite group of order n, there is exactly one subgroup for each divisor.

$\mathbf{G}$ is a cyclic group with order $[K : F] = n$. Since $k \mid n$, there is a subgroup I of order k in $\mathbf{G}$.

J. Normal Extensions and Normal Subgroups

Q1

$$I_1 \subseteq I_2 \subseteq K$$
$$\text{Gal}(I_2 : I_1) \cong \frac{\text{Gal}(K : I_1)}{\text{Gal}(K : I_2)}$$
$$I_2^* = \text{Gal}(K : I_2) \qquad I_1^* = \text{Gal}(K : I_1)$$

We conclude I_2^* is a normal subgroup of I_1^*.

Q2

$$h \in \mathrm{Gal}(K:F), g \in I^*$$
$$b = h(a)$$

$$\begin{aligned}[h \circ g \circ h^{-1}](b) &= h(g(h^{-1}(b))) \\ &= h(g(a)) \\ &= h(a) \\ &= b\end{aligned}$$

$$h(I)^* = \{\pi \in \mathbf{G} : \pi(b) = b \text{ for every } b \in h(I)\}$$

As we saw $h \circ g \circ h^{-1}$ leaves all elements $h(a) = b \in h(I)$ unchanged, and so $h \circ g \circ h^{-1} \in h(I)^*$.

$$\implies hI^*h^{-1} \subseteq h(I)^*$$

Q3

Observe that $hI^*h^{-1} \subseteq h(I)^* \implies I^* \subseteq h^{-1}h(I)^*h$ and h is a bijection.

Let $\bar{h} = h^{-1}, J = h(I)$ then observe that

$$\bar{h}J\bar{h}^{-1} \subseteq \bar{h}(J)^*$$

But $\bar{h}(h(J)) = I \implies \bar{h}(J)^* = I^*$ so

$$\begin{aligned} h^{-1}h(I)h &\subseteq I^* \\ \implies h(I) &\subseteq hI^*h^{-1} \\ \implies h(I) &= hI^*h^{-1} \qquad \text{using the previous question}\end{aligned}$$

Q4

By definition I_1^* and I_2^* are conjugate subgroups

$$\implies \exists g \in \mathbf{G} : I_2^* = gI_1^*g^{-1}$$

Let there be a $i \in \mathbf{G} : i(I_1) = I_2$

$$\begin{aligned} i(I_1)^* &= iI_1^*i^{-1} \\ &= I_2^*\end{aligned}$$

Likewise

$$I_2^* = iI_1^*i^{-1} \implies i(I_1)^* = I_2^* \implies i(I_1) = I_2$$

Q5

Definition of a normal subgroup is that for all $h \in I_1^*, g \in I_2^*$

$$hgh^{-1} \in I_2^*$$

Let $I_2 = I_1(c)$ with the minimum polynomial $p(x) : p(c) = 0$. Let $h(c) = c'$ where c' is another root of $p(x)$. $h \in I_1^*$ since I_1^* only fixes I_1 and $c \notin I_1$.

Now the operation $hgh^{-1} \in I_2^*$ by its normal property, and $hI_2^*h^{-1} = h(I_2)^*$.

I_2^* is a normal subgroup so $h(I_2)^* \subseteq I_2^*$ but h is bijection and preserves structure on intermediate fields, so $h(I_2)^* = I_2^* \implies h(I_2) = I_2$ from the previous answer.

$c \in I_2$, therefore $h(c) \in I_2$ and all other roots for $p(x)$.