MAU34106 - Galois Theory

Practice Sheet 3

Trinity College Dublin

Course homepage

These problems are just for practice, to help you warm up for the homework, and get more familiar with the material. I strongly encourage you to give them a try, as the best way to learn maths is through practice. They are arranged by theme, and roughly in order of difficulty within each theme, with the first few working as good warm-ups, and the remainder being of similar difficulty to the main exercise. You are welcome to email me if you have any questions about them. The solutions will be made available alongside the problems

---

Exercise 1 *Galois extensions of a quadratic field*

Find the splitting field K of x^3-7 over $\mathbb{Q}(\sqrt{3})$ and the Galois group $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{3})$. Using the Galois correspondence, determine all intermediate subfields $\mathbb{Q}(\sqrt{3}) \subset F \subset K$ along with the degrees

$$[F : \mathbb{Q}(\sqrt{3})], \quad [K : F].$$

Hint: $\mathrm{Gal}(K/\mathbb{Q})$ *must permute the roots of* $x^3 - 7$*, so embeds into* S_3

Solution 1

Let $\omega = e^{2\pi i/3}$ be a complex root of $x^3 - 1$. I claim $K = \mathbb{Q}(\sqrt{3}, \sqrt[3]{7}, \omega)$ is the splitting field of $x^3 - 7$ over $\mathbb{Q}(\sqrt{3})$. It is easy to see that $x^3 - 7$ splits in this field. Any splitting field must contain $\sqrt[3]{7}$ and $\sqrt[3]{7}\omega$, and hence must

contain $\omega = \frac{\sqrt[3]{7}\omega}{\sqrt[3]{7}}$. Thus, this must be the splitting field. While we could stop here, it is worth noting that this is basically the simplest presentation. As $[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] = 3$, $\sqrt[3]{7}$ cannot be an element of the quadratic extension $\mathbb{Q}(\sqrt{3})$ of $\mathbb{Q}$, and ω is complex, so cannot be an element of the real field $\mathbb{Q}(\sqrt{3}, \sqrt[3]{7})$. As such, $x^3 - 7$ is irreducible over $\mathbb{Q}(\sqrt{3})$ and the minimal polynomial $x^2 + x + 1$ of ω is irreducible over $\mathbb{Q}(\sqrt{3}, \sqrt[3]{7})$. This implies that

$$[K : \mathbb{Q}(\sqrt{3})] = [K : \mathbb{Q}(\sqrt{3}, \sqrt[3]{7})][\mathbb{Q}(\sqrt{3}, \sqrt[3]{7}) : \mathbb{Q}(\sqrt{3})] = 2 \times 3 = 6.$$

As $\mathbb{Q}(\sqrt{3})$ has characteristic 0, every splitting field is a Galois extension, so $G = \mathrm{Gal}(K/\mathbb{Q}(\sqrt{3}))$ is an order 6 group and is therefore equal to S_3. Considering the various permutations of $\sqrt[3]{7}$, $\sqrt[3]{7}\omega$ and $\sqrt[3]{7}\omega^2$, we find 6 automorphisms

$$\sigma_e : \begin{cases} \sqrt[3]{7} \mapsto \sqrt[3]{7} \\ \omega \mapsto \omega \end{cases} \quad , \quad \sigma_{(12)} : \begin{cases} \sqrt[3]{7} \mapsto \sqrt[3]{7}\omega \\ \omega \mapsto \omega^2 \end{cases}$$

$$\sigma_{(23)} : \begin{cases} \sqrt[3]{7} \mapsto \sqrt[3]{7} \\ \omega \mapsto \omega^2 \end{cases} \quad , \quad \sigma_{(13)} : \begin{cases} \sqrt[3]{7} \mapsto \sqrt[3]{7}\omega^2 \\ \omega \mapsto \omega^2 \end{cases}$$

$$\sigma_{(123)} : \begin{cases} \sqrt[3]{7} \mapsto \sqrt[3]{7}\omega \\ \omega \mapsto \omega \end{cases} \quad , \quad \sigma_{(132)} : \begin{cases} \sqrt[3]{7} \mapsto \sqrt[3]{7}\omega^2 \\ \omega \mapsto \omega \end{cases}$$

where we compute

$$\sigma_\bullet(\omega) = \sigma_\bullet\left(\frac{\sqrt[3]{7}\omega}{\sqrt[3]{7}}\right) = \frac{\sigma_\bullet(\sqrt[3]{7}\omega)}{\sigma_\bullet(\sqrt[3]{7})}$$

for each permutation of the roots.

The symmetric group has 4 non-trivial subgroups - 3 subgroups of order 2 and one subgroup of order 3:

$$\langle\sigma_{(12)}\rangle,\ \langle\sigma_{(23)}\rangle,\ \langle\sigma_{(13)}\rangle,\ \langle\sigma_{(123)}\rangle,$$

Thus there are 4 proper intermediate subfields, corresponding to the fixed subfields of each of these groups. We can write a generic element of K in the form

$$a + b\sqrt[3]{7} + c\sqrt[3]{49} + d\omega + e\sqrt[3]{7}\omega + f\sqrt[3]{49}\omega$$

where $a, b, c, d, e, f \in \mathbb{Q}(\sqrt{3})$. By explicitly computing elements fixed by the generators of each subgroup, we find the intermediate subfields

$$\begin{aligned} K^{\langle\sigma_{(12)}\rangle} &= \mathbb{Q}(\sqrt{3}, \sqrt[3]{7}\omega^2) \\ K^{\langle\sigma_{(23)}\rangle} &= \mathbb{Q}(\sqrt{3}, \sqrt[3]{7}) \\ K^{\langle\sigma_{(13)}\rangle} &= \mathbb{Q}(\sqrt{3}, \sqrt[3]{7}\omega) \\ K^{\langle\sigma_{(123)}\rangle} &= \mathbb{Q}(\sqrt{3}, \omega) \end{aligned}$$

and Galois correspondence tells us the degrees are

$$\begin{aligned} [K : K^{\langle\sigma_{(12)}\rangle}] = |\langle\sigma_{(12)}\rangle| = 2, \quad [K^{\langle\sigma_{(12)}\rangle} : \mathbb{Q}(\sqrt{3})] = \frac{|S_3|}{|\langle\sigma_{(12)}\rangle|} = 3 \\ [K : K^{\langle\sigma_{(23)}\rangle}] = |\langle\sigma_{(23)}\rangle| = 2, \quad [K^{\langle\sigma_{(23)}\rangle} : \mathbb{Q}(\sqrt{3})] = \frac{|S_3|}{|\langle\sigma_{(23)}\rangle|} = 3 \\ [K : K^{\langle\sigma_{(13)}\rangle}] = |\langle\sigma_{(13)}\rangle| = 2, \quad [K^{\langle\sigma_{(13)}\rangle} : \mathbb{Q}(\sqrt{3})] = \frac{|S_3|}{|\langle\sigma_{(13)}\rangle|} = 3 \\ [K : K^{\langle\sigma_{(123)}\rangle}] = |\langle\sigma_{(123)}\rangle| = 3, \quad [K^{\langle\sigma_{(123)}\rangle} : \mathbb{Q}(\sqrt{3})] = \frac{|S_3|}{|\langle\sigma_{(123)}\rangle|} = 2 \end{aligned}$$

Exercise 2 *Calculus in an algebra course?!?*

Let $f(x) = x^3+4x+1$ be an irreducible polynomial, and let $K = \mathbb{Q}[x]/(f(x))$. Is K a separable extension of $\mathbb{Q}$? A normal extension? A Galois extension?

Hint: How many real roots does $f(x)$ have? Can it split if we adjoint one root to $\mathbb{Q}$?

Solution 2

As $\mathbb{Q}$ has characteristic 0, $K/\mathbb{Q}$ is separable.

As $f(x)$ is a cubic, it has at least one real root. As $f'(x) = 3x^2 + 4 > 0$, $f(x)$ is strictly increasing, and so has exactly one real root α. We have that $K \cong \mathbb{Q}(\alpha)$, which cannot contain the two complex roots, so $f(x)$ cannot split as a product of linear factors in K. Hence $K/\mathbb{Q}$ is not normal, or Galois.

Exercise 3 *Linear independence of square roots*

Let $K = \mathbb{Q}(\sqrt{10}, \sqrt{38})$.

1. Show that $K/\mathbb{Q}$ is a Galois extension.
2. Show that $[K : \mathbb{Q}] = 4$.
3. Describe explicitly the elements of $\mathrm{Gal}(K/\mathbb{Q})$. To which group is $\mathrm{Gal}(K/\mathbb{Q})$ isomorphic.
4. Sketch the diagram showing all intermediate subfields $\mathbb{Q} \subset F \subset K$, ordered by inclusion. Clearly indicate to which subgroup they correspond.
5. Using your knowledge of the intermediate subfields, determine whether $\sqrt{15} \in K$.

Solution 3

1. K is the splitting field of $f(x) = (x^2 - 10)(x^2 - 38)$, and is therefore normal over $\mathbb{Q}$. Over a field of characteristic 0, this implies $K/\mathbb{Q}$ is Galois.
2. As $\frac{38}{10} = \frac{17}{5}$ is not a square in $\mathbb{Q}$, $x^2 - 10$ is irreducible over $\mathbb{Q}(\sqrt{38})$. Thus

   $$[\mathbb{Q}(\sqrt{10}, \sqrt{38}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{10}, \sqrt{38}) : \mathbb{Q}(\sqrt{38})][\mathbb{Q}(\sqrt{38}) : \mathbb{Q}] = 2{\times}2 = 4.$$

3. As $K/\mathbb{Q}$ is a Galois extension $G = \mathrm{Gal}(K/\mathbb{Q})$ is a group of order 4. Knowing that elements of G must send roots of $x^2 - 10$ to roots of $x^2 - 10$ and roots of $x^2 - 38$ to roots of $x^2 - 38$, there are exactly 4 possible automorphisms, and so the Galois group must consist of

   $$id : \begin{cases} \sqrt{10} \mapsto \sqrt{10} \\ \sqrt{38} \mapsto \sqrt{38} \end{cases} \quad , \quad \sigma : \begin{cases} \sqrt{10} \mapsto -\sqrt{10} \\ \sqrt{38} \mapsto \sqrt{38} \end{cases}$$
   $$\tau : \begin{cases} \sqrt{10} \mapsto \sqrt{10} \\ \sqrt{38} \mapsto -\sqrt{38} \end{cases} \quad , \quad \mu : \begin{cases} \sqrt{10} \mapsto -\sqrt{10} \\ \sqrt{38} \mapsto -\sqrt{38} \end{cases}$$

   and is clearly isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$.

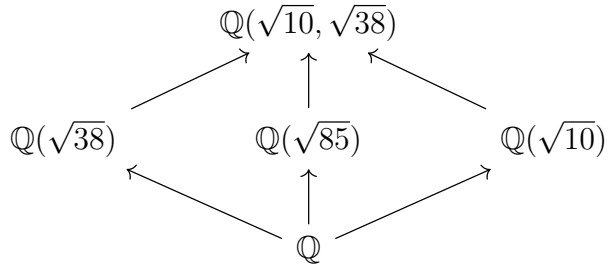
4. The Galois group has 3 non-trivial subgroups, and so there are exactly 3 non-trivial intermediate subfields, shown in the diagram below, where

$$\mathbb{Q}(\sqrt{38}) = K^{\sigma},\ \mathbb{Q}(\sqrt{85}) = K^{\mu},\ \mathbb{Q}(\sqrt{38}) = K^{\tau}$$

which we can find by computing fixed elements of each subfield explicitly by looking at the action on an arbitrary element of K:

$$a + b\sqrt{10} + c\sqrt{38} + d\sqrt{85}.$$

5. If $\sqrt{15} \in K$, then $\mathbb{Q}(\sqrt{15})$ is an intermediate subfield. As it is a quadratic extension, it must be equal to one of $\mathbb{Q}(\sqrt{10})$, $\mathbb{Q}(\sqrt{38})$, $\mathbb{Q}(\sqrt{85})$. But $x^2 - 15$ is irreducible over each of these fields, as $\frac{15}{10}$, $\frac{15}{38}$, and $\frac{15}{85}$ are not squares over $\mathbb{Q}$.



Exercise 4 *Have I mentioned pentagons enough yet?*

Let $\zeta = e^{2\pi i/5}$ be a primitive root of unity, and let $K = \mathbb{Q}(\zeta)$. This is a Galois extension of $\mathbb{Q}$, and we let $G = \mathrm{Gal}(K/\mathbb{Q})$. Also define

$$c = \frac{\zeta + \overline{\zeta}}{2} = \frac{\zeta + \zeta^{-1}}{2} = \cos(2\pi/5).$$

1. We know that the minimal polynomial of ζ is the cyclotomic polynomial $\Phi_5(x)$. Use the recursion to determine $\Phi_5(x)$.

2. We have seen that G is a cyclic group. Determine its order and find an explicit generator of G.

3. Hence or otherwise show that $c \notin \mathbb{Q}$.

   Hint: Elements of $\mathbb{Q}$ are fixed by G. Do some numerics on the orbit of c.

4. Using the Galois correspondence, determine all intermediate subfields $\mathbb{Q} \subset F \subset K$.

5. Determine the minimal polynomial of c over $\mathbb{Q}$. Hence determine c exactly.

   Hint: Recall Corollary 5.15

6. Use the Galois correspondence to determine $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(c))$, and hence determine the minimal polynomial of ζ over $\mathbb{Q}(c)$. Use this to give an exact expression for ζ.

Solution 4

1. Since 5 is prime

$$x^5 - 1 = \Phi_5(x)\Phi_1(x) = \Phi_5(x)(x-1)$$

   and hence

$$\Phi_5(x) = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1$$

2. Since $K/\mathbb{Q}$ is Galois, $|G| = [K : \mathbb{Q}] = 4$. Every element of G is determined by its action on ζ, and must act transitively on the set of roots of $\Phi_5(x)$. Hence, there is an automorphism σ such that $\sigma(\zeta) = \zeta^2$. We can check that

$$\begin{aligned}\sigma^2(\zeta) &= \sigma(\zeta^2) = (\sigma(\zeta))^2 = \zeta^4,\\ \sigma^3(\zeta) &= \sigma(\sigma^2(\zeta)) = \sigma(\zeta^4) = (\zeta^2)^4 = \zeta^8 = \zeta^3\end{aligned}$$

   and $\sigma^4(\zeta) = \zeta$. This gives all four automorphisms, and so σ is a generator.

3. According to the Galois correspondence, $c \in \mathbb{Q}$ if and only if c is fixed by G, in particular if c is fixed by σ. We can check

$$\sigma(c) = \frac{\sigma(\zeta) + \sigma(\zeta^{-1})}{2} = \frac{\zeta^2 + \zeta^{-2}}{2} = \cos(4\pi/5) \approx -0.8$$

   while $c \approx 0.3$, so c is not fixed by the Galois group and is therefore not rational.

4. There is only one possible non-trivial intermediate subfield, as $G \cong \mathbb{Z}/4\mathbb{Z}$ has only one non-trivial subgroup, generated by σ^2. Writing elements of K in the form

$$a + b\zeta + c\zeta^2 + d\zeta^3$$

we see that elements fixed by σ^2 are those such that

$$\begin{aligned} a + b\zeta + c\zeta^2 + d\zeta^3 &= \sigma^2(a + b\zeta + c\zeta^2 + d\zeta^3) \\ &= a + b\zeta^4 + c\zeta^3 + d\zeta \\ &= a + b(-1 - \zeta - \zeta^2 - \zeta^3 - \zeta) + c\zeta^3 + d\zeta^2 \end{aligned}$$

as

$$\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0.$$

Comparing coefficients, we must have

$$b = 0,\ c = d$$

and so the only intermediate subfield is

$$\mathbb{Q}(\zeta^2 + \zeta^3) = \mathbb{Q}(\cos(4\pi/5)).$$

Since

$$c + \cos(4\pi/5) = \frac{\zeta + \zeta^2 + \zeta^3 + \zeta^4}{2} = \frac{-1}{2}$$

we must also have

$$\mathbb{Q}(\cos(4\pi/5)) = \mathbb{Q}(c).$$

Alternatively we could also conclude this by noting that $\mathbb{Q}(c) \neq \mathbb{Q}$ and $\mathbb{Q}(\zeta) \neq \mathbb{Q}(c)$, so $\mathbb{Q}(c)$ must be the unique intermediate subfield.

5. Corollary 5.15 tells us that the minimal polynomial of c is

$$\prod_{\beta \in G \cdot c} (x - \beta)$$

where

$$G \cdot c = \{g(c) \mid g \in G\}.$$

We compute

$$\{c, \sigma(c), \sigma^2(c), \sigma^3(c)\} = \{c, \sigma(c)\}$$

as sets, and so the minimal polynomial of c is

$$\begin{aligned}(x-c)(x-\sigma(c)) &= \left(x-\frac{\zeta+\zeta^4}{2}\right)\left(x-\frac{\zeta^2+\zeta^3}{2}\right)\\ &= x^2-\frac{\zeta+\zeta^2+\zeta^3+\zeta^4}{2}x+\frac{(\zeta+\zeta^4)(\zeta^2+\zeta^3)}{4}\\ &= x^2-\frac{(-1)}{2}x+\frac{\zeta^3+\zeta^4+\zeta^6+\zeta^7}{4}\\ &= x^2+\frac{1}{2}x-\frac{1}{4}.\end{aligned}$$

Hence

$$c=\frac{-1\pm\sqrt{5}}{2}.$$

As $c>0$, we must have $c=\frac{-1+\sqrt{5}}{2}$.

6. As $\mathbb{Q}(c)$ is fixed by the subgroup generated by σ^2, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(c)) = \langle\sigma^2\rangle$. The orbit of ζ under the action of this group is the set

$$\{\zeta,\sigma^2(\zeta)\}=\{\zeta,\zeta^4\}$$

and hence the minimal polynomial of ζ over $\mathbb{Q}(c)$ is

$$(x-\zeta)(x-\zeta^4)=x-2c+1.$$

Hence ζ is one of

$$\frac{2c\pm\sqrt{4c^2-4}}{2}$$

which is more explicitly

$$\frac{-1+\sqrt{5}\pm i\sqrt{10+2\sqrt{5}}}{4}.$$

As $\sin(2\pi/5)>0$, ζ has positive imaginary part and hence

$$\zeta=\frac{-1+\sqrt{5}+i\sqrt{10+2\sqrt{5}}}{4}.$$

Exercise 5 *Our favourite form of extension*

Let L/K be a Galois extension with Galois group $G=\{g_1,\ldots,g_n\}$. Let $a\in K$, and show that $L=K(a)$ if and only if $g_1(a)$, $g_2(a)$,..., $g_n(a)$ are distinct elements of L.

Solution 5

Suppose $L = K(a)$. Then

$$n = |G| = [L : K] = [K(a) : K] = \deg_K(a)$$

and so the minimal polynomial $f(x)$ of a over K has degree n. As L/K is Galois, it is separable, and so the minimal polynomial of a has n distinct roots. The Galois group acts transitively on the roots of $f(x)$, and so

$$|\{g_1(a), g_2(a), \ldots, g_n(a)\}| = n$$

as the set must contain every root of $f(x)$. Thus $g_1(a)$,...,$g_n(a)$ are all distinct elements of L.

Conversely, if $g_1(a)$,...,$g_n(a)$ are all distinct elements of L, and so the minimal polynomial of a over K is

$$f(x) = \prod_{j=1}^{n}(x - g_j(a)).$$

In particular, a is algebraic of degree n, and so $[K(a) : K] = n$. But since L/K is Galois, $[L : K] = |G| = n$, we have that

$$[L : K(a)] = \frac{[L : K]}{[K(a) : K]} = 1$$

and so $L = K(a)$.

Exercise 6 *A past exam question*

Let $f(x) = x^4 - 5x^2 + 1$. This is irreducible over $\mathbb{Q}$, and has a root $\alpha \in \mathbb{C}$. Let $K = \mathbb{Q}(\alpha)$. You should not need to compute α explicitly in any of the following.

1. Express the 4 roots of $f(x)$ in terms of α

   Hint: Consider $\frac{1}{\alpha}$

2. Show that $K/\mathbb{Q}$ is a Galois extension

3. Show that $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ and explicitly describe its action on α

4. Draw a diagram showing all intermediate subfields $\mathbb{Q} \subset F \subset K$, and give an explicit form for each such subfield.

5. Show that $K = \mathbb{Q}(\sqrt{3}, \sqrt{7})$

Solution 6

1. As $f(-x) = f(x)$, $-\alpha$ is also a root of $f(x)$. Since the product of the roots is 1, $\alpha \neq 0$, so $-\alpha \neq 0$. We also have that $f(x^{-1}) = x^{-4} f(x)$, and so α^{-1} is also a root of $f(x)$. As $f(1) \neq 0$ and $f(-1) \neq 0$, neither ± 1 are roots. As such $\alpha \neq \alpha^{-1}$. We can similarly check that $\alpha^{-1} \neq -\alpha$, as neither $\pm i$ are roots of $f(x)$. This gives a third root of $f(x)$. A similar argument shows that the fourth root is $-\alpha^{-1}$.

2. Clearly K contains all the roots of $f(x)$, so K is the splitting field of $f(x)$ over $\mathbb{Q}$. As $\mathbb{Q}$ has characteristic 0, this implies that $K/\mathbb{Q}$ is Galois.

3. We must have that
$$[K : \mathbb{Q}] = \deg f(x) = 4$$
and since it is Galois, the Galois group is of order 4. As the Galois group acts transitively on the roots of $f(x)$, and is completely determined by its action on α, we find that the 4 elements of the Galois group must be
$$\begin{aligned} id : \alpha \mapsto \alpha, \quad \sigma : \alpha \mapsto -\alpha \\ \tau : \alpha \mapsto \alpha^{-1}, \quad \mu : \alpha \mapsto -\alpha^{-1}. \end{aligned}$$
As each of these has order 2, we must have that
$$\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

4. The inclusion diagram is given below, showing the three non-trivial intermediate subfields, corresponding to the subgroups generated by σ, τ, and μ respectively. As each of these is of order and index 2, we must have that
$$[K^\sigma : \mathbb{Q}] = [K^\tau : \mathbb{Q}] = [K^\mu : \mathbb{Q}] = 2$$
and so to describe them, it suffices to find a single irrational element of K fixed by the appropriate automorphism.

We note that

$$\sigma(\alpha^2) = (\sigma(\alpha))^2 = (-\alpha^2) = \alpha^2.$$

As α^2 is not rational, we therefore have

$$K^\sigma = \mathbb{Q}(\alpha^2).$$

Furthermore, α^2 is a root of $f(\sqrt{x}) = x^2 - 5x + 1$, so we can compute

$$\alpha^2 = \frac{5 \pm \sqrt{21}}{2}$$

and so $\mathbb{Q}(\sqrt{21}) \subset K^\sigma$. As both of these are of degree 2, we therefore have

$$K^\sigma = \mathbb{Q}(\sqrt{21}).$$

We next note that

$$\tau(\alpha + \alpha^{-1}) = \alpha^{-1} + \alpha$$

and cannot be rational (as otherwise α would satisfy a quadratic equation), we have that

$$K^\tau = \mathbb{Q}(\alpha + \alpha^{-1}).$$

We must have that $\alpha + \alpha^{-1}$ satisfies a quadratic, so considering

$$(\alpha + \alpha^{-1})^2 = \alpha^2 + 2 + \alpha^{-2} = \frac{\alpha^4 + 2\alpha^2 + 1}{\alpha^2} = \frac{5\alpha^{-}1 + 2\alpha^2 + 1}{\alpha^2} = 7.$$

Thus, $\mathbb{Q}(\sqrt{7}) \subset K^\tau$. These are both extensions of degree 2 of $\mathbb{Q}$, and so we must have

$$K^\tau = \mathbb{Q}(\sqrt{7})$$

Finally,

$$\mu(\alpha - \alpha^{-1}) = -\alpha^{-1} + \alpha$$

is fixed by μ, and irrational. Thus

$$K^\mu = \mathbb{Q}(\alpha - \alpha^{-1})$$

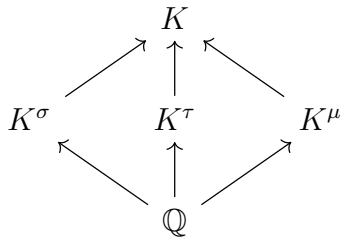
Similarly to the last paragraph

$$(\alpha - \alpha^{-1})^2 = \frac{5\alpha^2 - 1 - 2\alpha^2 + 1}{\alpha^2} = 3$$

and so $\mathbb{Q}(\sqrt{3}) \subset K^\mu$. For reasons of degree

$$K^\mu = \mathbb{Q}(\sqrt{3}).$$

5. Since $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{7})$ are subfields of K, $\mathbb{Q}(\sqrt{3},\sqrt{7})$ is a subfield of K. As the only field in the diagram containing both $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{7})$ is K, the Galois correspondence tells us that we must have $K = \mathbb{Q}(\sqrt{3},\sqrt{7})$.



Exercise 7 *Algebra in a calculus course?!?*

This exercise is not representative of an exam question, and is essentially entirely plagiarised from Nicolas Mascot's version of this course, but is really neat. Over the course of your calculus courses, you likely developed an implicit intuition for simple cases of Bioche's rules, which give guidelines for substitutions to make in order to reduce the integral of a rational function of trigonometic functions to an integral of a rational function of a variable u. Here, we attempt to give a Galois-theoretic motivation for these rules.

Let $s := \sin(x)$ and $c := \cos(x)$ throughout, and consider the field of rational trigonometric functions $\mathbb{C}(s,c)$ over the complex numbers, which include expressions like

$$\frac{s^3c + is - 3}{s + c + 17} = \frac{\sin^3(x)\cos(x) + i\sin(x) - 3}{\sin(x) + \cos(x) + 17}.$$

This has two distinguished subfields $\mathbb{C}(c)$ and $\mathbb{C}(s)$ consisting of rational functions in $\cos(x)$ and $\sin(x)$ respectively. We let $K = \mathbb{C}(c) \cap \mathbb{C}(s)$ be the intersection, which contains elements such as 1 and

$$\cos(2x) = 2c^2 - 1 = 1 - 2s^2.$$

We define two automorphisms of $\mathbb{C}(s,c)$ by

$$\mu : f(x) \mapsto f(-x), \quad \tau : f(x) \mapsto f(x + \pi)$$

1. Show that μ and τ generate a group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$.

2. Show that the four inclusions

$$K \subset \mathbb{C}(c),\ K \subset \mathbb{C}(s),\ \mathbb{C}(c) \subset \mathbb{C}(s,c),\ \mathbb{C}(s) \subset \mathbb{C}(s,c)$$

are strict inclusions.

3. Show that each of these four extensions is an algebraic extension of degree 2.

4. Show that $K = \mathbb{C}(c_2)$, where $c_2 = \cos(2x)$.

5. Show that $\mathbb{C}(s,c)/K$ is Galois, and show that its Galois group is generated by μ and τ.

6. Determine the minimal polynomials of $t = \tan(x) = \frac{s}{c}$ and $s_2 = \sin(2x) = 2sc$ over K.

7. Using the Galois correspondence, determine all intermediate subfields $K \subset F \subset \mathbb{C}(s,c)$ and draw an inclusion diagram

8. Determine where the fields $\mathbb{C}(t)$, $\mathbb{C}(s_2, c_2)$, and $\mathbb{C}(s_2)$ lie in this diagram

9. Ponder how this suggests Bioche's rules

Solution 7

1. This is a direct calculation:

$$\mu^2 = \tau^2 = e$$

where e denote the identity automorphism. We also have that

$$\mu\tau = \tau\mu$$

and so we have an abelian group generated by two elements of order 2. The only such group is $(\mathbb{Z}/2\mathbb{Z})^2$.

2. If $\mathbb{C}(c) = K$, then $\mathbb{C}(c) \subset \mathbb{C}(s)$, and so we can write

$$c = f(s)$$

for some rational function $f(z) \in \mathbb{C}(z)$. This is a statement about functions:

$$\cos(x) = f(\sin(x))$$

and this must hold for all $x \in \mathbb{C}$. By taking $x = 0$,$x = \pi$, we must have $f(0) = 1$ and $f(0) = -1$, so this cannot hold. Similarly, if $\mathbb{C}(s) = K$, then $\mathbb{C}(s) \subset \mathbb{C}(c)$, and the same argument holds.

To see that $\mathbb{C}(s) \neq \mathbb{C}(s, c)$, we note that if these are equal, then $\cos(x) = f(\sin(x))$ for some rational function $f(z) \in \mathbb{C}(z)$, and the same arguments again shows that this cannot hold. Similarly $\mathbb{C}(c) \neq \mathbb{C}(s, c)$.

Alternatively, note that every element of $\mathbb{C}(c)$ is an even function, and s is an odd function, so cannot be an element of $\mathbb{C}(c)$, and similarly $\mathbb{C}(s)$ cannot contain c (or c_2).

3. As $2c^2 - 1 \in K$, $[\mathbb{C}(c) : K] \leq 2$. It cannot be 1, as the inclusions are strict, so it must be 2. Similarly, $2s^2 - 1 \in K$, and the same argument shows $[\mathbb{C}(s) : K] = 2$.

   Finally, as $s^2 + c^2 = 1$, we must have that

   $$[\mathbb{C}(s, c) : \mathbb{C}(s)] \leq 2 \geq [\mathbb{C}(s, c) : \mathbb{C}(c)].$$

   In fact, we must have equality, as the inclusions are strict.

4. We know that $\mathbb{C}(c_2) \subset K$, and so by tower law

   $$[K : \mathbb{C}(c_2)] = \frac{[\mathbb{C}(c) : \mathbb{C}(c_2)]}{[\mathbb{C}(c) : K]} = \frac{[\mathbb{C}(c) : \mathbb{C}(c_2)]}{2}.$$

   Since $2c^2 - 1 = c_2$, $[\mathbb{C}(c) : \mathbb{C}(c_2)] \leq 2$, and so

   $$[K : \mathbb{C}(c_2)] \leq 1 \quad \Rightarrow \quad [K : \mathbb{C}(c_2)] = 1.$$

   Thus, they are equal.

5. By tower law

   $$[\mathbb{C}(s, c) : K] = [\mathbb{C}(s, c) : \mathbb{C}(c)][\mathbb{C}(c) : K] = 2 \times 2 = 4$$

   and so

   $$|\operatorname{Gal}(\mathbb{C}(s, c)/K)| \leq 4.$$

We have 4 automorphisms of $\mathbb{C}(s,c)$ in e, μ, τ and $\mu\tau$, each of which fix $K = \mathbb{C}(c_2)$:

$$\mu(\cos(2x)) = \cos(-2x) = \cos(2x),\ \tau(\cos(2x)) = \cos(2x+2\pi) = \cos(2x).$$

Hence these are all elements of $\mathrm{Gal}(\mathbb{C}(s,c)/K)$, and so

$$|\operatorname{Gal}(\mathbb{C}(s,c)/K)| \geq 4.$$

Therefore the Galois group has order 4, and so the extension is Galois. (Recall that an extension is Galois if and only if the order of the Galois group is equal to the degree of the extension.)

6. The Galois orbit of t is

$$\{t, \mu(t), \tau(t), \mu\tau(t)\} = \{t, -t, t, -t\}$$

and so the minimal polynomial is

$$(x-t)(x+t) = x^2 - t^2 = x^2 - \frac{s^2}{c^2} = \frac{1-c_2}{1+c_2}.$$

Similarly, the Galois orbit of $s_2 = 2sc$ is

$$\{s_2, -s_2, s_2, -s_2\}$$

and so the minimal polynomial is

$$x^2 - s_2^2 = x^2 - (1 - c_2^2).$$

7. The only non-trivial subgroups of the Galois group are $\langle\mu\rangle$, $\langle\tau\rangle$, and $\langle\mu\tau\rangle$, and so we have three non-trivial intermediate subfields, with inclusions as shown in the diagram below. The fixed subfields are computed as follows.

We know that, for each subgroup H,

$$[\mathbb{C}(s,c)^H : K] = \frac{|(\mathbb{Z}/2\mathbb{Z})^2|}{|H|} = \frac{4}{2} = 2.$$

The element c is fixed by μ and so $\mathbb{C}(c) \subset \mathbb{C}(s,c)^\mu$, and must be equal for reasons of degree.

Similarly, , the element s is fixed by $\mu\tau$, and so $\mathbb{C}(s,c)^{\mu\tau} = \mathbb{C}(s)$.

Finally, we have seen that t is fixed by τ. As $c_2 = \frac{1}{1+t^2}$, $K \subset \mathbb{C}(t)$, so it is an intermediate subfield fixed by τ. Hence $\mathbb{C}(t) \subset \mathbb{C}(s,c)^\tau$. Since $\mu(t) \neq t$, t cannot be an element of K, and so we must have that $\mathbb{C}(t) = \mathbb{C}(s,c)^\tau$.

We also have that s_2 is fixed by τ, but not μ, so we must actually have

$$\mathbb{C}(t) = \mathbb{C}(s,c)^\tau = K(s_2) = \mathbb{C}(s_2, c_2).$$

(We cannot take $\mathbb{C}(s_2)$, as it does not contain $K = \mathbb{C}(c_2)$, so it is not an intermediate subfield.)

8. We have already done this as part of the previous part! There was a bit of a trap here, as $\mathbb{C}(s_2)$ does not appear in the diagram, since it does not contain K.

9. Suppose $f(x) \in \mathbb{C}(s,c)$. If $f(-x) = -f(x)$, then

$$g(x) := \frac{-f(x)}{\sin(x)}$$

is invariant under μ and so $g(x) \in \mathbb{C}(c)$. Thus there exists a rational function $r(z)$ such that $g(x) = r(\cos(x))$. Letting $u = \cos(x)$, then

$$f(x)dx = r(\cos(x))(-\sin(x))dx = r(\cos(x))d\cos(x) = r(u)du.$$

Similarly, if $f(\pi - x) = -f(x)$, then

$$g(x) := \frac{f(x)}{\cos(x)}$$

is invariant under $\mu\tau$ and so $g(x) \in \mathbb{C}(s)$. Thus, there exists a rational function $r(z) \in \mathbb{C}(z)$ such that $g(x) = r(\sin(x))$. Letting $u = \sin(x)$, we find

$$f(x)dx = r(\sin(x))\cos(x)dx = r(\sin(x))d\sin(x) = r(u)du.$$

If $f(x + \pi) = -f(x)$, then

$$g(x) := \cos^2(x)f(x)$$

is invariant under τ and so $g(x) \in \mathbb{C}(t)$. Thus, there exists a rational function $r(z) \in \mathbb{C}(z)$ such that $g(x) = r(\tan(x))$. Letting $u = \tan(x)$, we find

$$f(x)dx = r(\tan(x)) \sec^2(x)dxr(\tan(x))d\tan(x) = r(u)du.$$

If two of the above properties hold, then

$$g(x) := \frac{-f(x)}{2\sin(2x)}$$

is invariant under the entire Galois group, and so $g(x) \in K$. Thus, there exists a rational function $r(z) \in \mathbb{C}(z)$ such that $g(x) = r(\cos(2x))$. Letting $u = \cos(2x)$, we find

$$f(x)dx = -2r(\cos(2x)) \sin(2x)dx = r(\cos(2x)d\cos(2x) = r(u)du$$

This explains 4 of the 5 Bioche rules!