# 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* $S_3$

## 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* $\mathbb{Q}$*?*

## 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 $\sqrt{15} \in K$.

## 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 $\zeta$ 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 $\zeta$ over $\mathbb{Q}(c)$. Use this to give an exact expression for $\zeta$.

## 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 $L$.

## 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 $\alpha$ explicitly in any of the following.

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

   *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 $\alpha$

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 $K = \mathbb{Q}(\sqrt{3}, \sqrt{7})$

## 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 $\mu$ and $\tau$ 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 $\mu$ and $\tau$.
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