MAU34106 - Galois Theory

Practice Sheet 2

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 *Abstract computations*

1. Show that $x^3 - 2x - 2$ is irreducible over $\mathbb{Q}$
2. Denote by α a root of of the polynomial. Express each of

$$\frac{1}{\alpha}, \quad \frac{1}{1+\alpha}, \quad \frac{1}{1+\alpha^2}$$

in the form

$$a + b\alpha + c\alpha^2, \quad a, b, c \in \mathbb{Q}.$$

Solution 1

1. This is irreducible by Eisenstein's criterion for $p = 2$.

2. We first want to find a, b, c such that

$$(a + b\alpha + c\alpha^2)\alpha = 1$$

or equivalently

$$1 = a\alpha + b\alpha^2 + c\alpha^3 = a\alpha + b\alpha^2 + c(2\alpha + 2)$$

as $\alpha^3 = 2\alpha + 2$. As $1, \alpha, \alpha^2$ form a basis, we can compare coefficients to find

$$\begin{aligned} 1 &= 2c \\ 0 &= a + 2c \\ 0 &= b \end{aligned}$$

and hence

$$a = -1,\ b = 0,\ c = \frac{1}{2} \quad \Rightarrow \quad \frac{1}{\alpha} = -1 + \frac{\alpha^2}{2}.$$

We similarly can find $a, b, c \in \mathbb{Q}$ such that

$$(a + b\alpha + c\alpha^2)(1 + \alpha) = 1$$

and hence

$$\begin{aligned} a + 2c &= 1 \\ b + a + 2c &= 0 \\ b + c &= 0 \end{aligned}$$

which implies that

$$\frac{1}{1 + \alpha} = -1 - \alpha + \alpha^2.$$

Finally, we can find $a, b, c \in \mathbb{Q}$ such that

$$(a + b\alpha + c\alpha^2)(1 + \alpha^2) = 1$$

and hence, using $\alpha^4 = 2\alpha^2 + 2\alpha$, we must have

$$\begin{aligned} a + 2b &= 1 \\ 3b + 2c &= 0 \\ a + 2c &= 0 \end{aligned}$$

which implies that

$$\frac{1}{1 + \alpha^2} = \frac{3}{5} + \frac{\alpha}{5} - \frac{3\alpha^2}{10}?$$

Exercise 2 *Finding splitting fields*

1. Compute the degree of the splitting field of $x^4 - 6$ over $\mathbb{Q}$ and give a nice $\mathbb{Q}$-basis for the splitting field.

2. Compute the degree of the splitting field of $x^{12} - 1$ over $\mathbb{Q}$ and give a nice $\mathbb{Q}$-basis.

3. Show that the splitting fields of $x^{12} - 1$ and $(x^4 - 1)(x^3 - 1)$ coincide.

Solution 2

The solution to both of these problems is essentially to add elements to $\mathbb{Q}$ until we obtain a field in which the polynomial splits, and then verify that this field is minimal. The easiest place to start is, if possible, solving the equation in $\mathbb{C}$.

1. We can easily check that in $\mathbb{C}$

$$x^4 - 6 = (x - \sqrt[4]{6})(x + \sqrt[4]{6})(x - \sqrt[4]{6}i)(x + \sqrt[4]{6}i)$$

and so $x^4 - 6$ splits in

$$\mathbb{Q}(\sqrt[4]{6}, \sqrt[4]{6}i) = \mathbb{Q}(\sqrt[4]{6}, i)$$

To see that it is minimal, note that the splitting field (viewed as a subfield of $\mathbb{C}$) must contain $\sqrt[4]{6}$ and $\frac{\sqrt[4]{6}i}{\sqrt[4]{6}} = i$, so $\mathbb{Q}(\sqrt[4]{6}, i)$ is a subfield of the splitting field. Hence $\mathbb{Q}(\sqrt[4]{6}, i)$ is the splitting field.

To compute the degree, we apply tower law

$$[\mathbb{Q}(\sqrt[4]{6}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{6}, i), \mathbb{Q}(\sqrt[4]{6})][\mathbb{Q}(\sqrt[4]{6}) : \mathbb{Q}].$$

As $x^4 - 6$ is the minimal polynomial of $\sqrt[4]{6}$ over $\mathbb{Q}$, we must have that

$$[\mathbb{Q}(\sqrt[4]{6}) : \mathbb{Q}] = 4$$

Similarly, $x^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}(\sqrt[4]{6})$, as $\mathbb{Q}(\sqrt[4]{6})$ is a subfield of the reals and $x^2 + 1$ has no real roots. Hence

$$[\mathbb{Q}(\sqrt[4]{6}, i), \mathbb{Q}(\sqrt[4]{6})] = 2$$

and so

$$[\mathbb{Q}(\sqrt[4]{6}, i), \mathbb{Q}] = 8$$

with a basis given by

$$\{1, \sqrt[4]{6}, \sqrt{6}, \sqrt{6}\sqrt[4]{6}, i, \sqrt[4]{6}i, \sqrt{6}i, \sqrt{6}\sqrt[4]{6}i\}$$

2. First, we note that the roots of $x^{12} - 1$ in $\mathbb{C}$ are

$$\{\zeta^k \mid 0 \leq k < 12$$

where $\zeta = e^{\frac{2\pi i}{12}} = e^{\frac{\pi i}{6}}$. Thus, $x^{12} - 1$ splits in $\mathbb{Q}(\zeta)$, and this is clearly minimal, as the splitting field must contain ζ. Thus, we just need to compute the degree of this extension, which will be the degree of the minimal polynomial of ζ. Note that

$$\zeta^6 = e^{\pi i} = -1$$

and so ζ is a root of $x^6 + 1$. This splits further as

$$x^6 + 1 = (x^2 + 1)(x^4 - x^2 + 1)$$

The roots of $x^2 + 1$ are $\pm i$, so ζ is a root of $x^4 - x^2 + 1$. This has no real roots, and we can check that there is no quadratic factorisation over the rationals

$$x^4 - x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

It is therefore the minimal polynomial, so

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$$

with a basis given by

$$\{1, \zeta, \zeta^2, \zeta^3\}.$$

3. Denote by $\omega = e^{\frac{2\pi i}{3}}$ and i two of the complex roots of $(x^3 - 1)(x^4 - 1)$. It is easy to check that this polynomial splits as a product of linear factors in $\mathbb{Q}(\omega, i)$. Furthermore, note that

$$\omega = \zeta^4, \quad i = \zeta^3$$

and so

$$\mathbb{Q}(\omega, i) = \mathbb{Q}(\zeta).$$

We claim that $(x^3-1)(x^4-1)$ cannot split in any smaller field. Indeed, the splitting field of this polynomial must contain

$$\frac{\omega}{i} = e^{\frac{2\pi i}{3} - \frac{\pi i}{2}} = e^{\frac{\pi i}{6} = \zeta}$$

and hence must contain $\mathbb{Q}(\zeta)$. Therefore, the splitting field of $(x^3 - 1)(x^4 - 1)$ is $\mathbb{Q}(\zeta)$.

Exercise 3 *Modelling* $\mathbb{F}_8$

Let $K = \mathbb{F}_2[x]/(x^3 + x^2 + 1)$ and $L = \mathbb{F}_2[y]/(y^3 + y + 1)$.

1. Show that both K and L are fields.
2. Determine the number of elements of K and L.
3. By giving an explicit map, show that $K \cong L$

   Hint: What is the minimal polynomial of $x + 1$ *over* $\mathbb{F}_2$.

Solution 3

1. Recall that the maximal ideal of $\mathbb{F}_2[x]$ correspond to irreducible polynomials. As the quotient of a ring by a maximal ideal is a field, it suffices to show that $x^3 + x^2 + 1$ and $x^3 + x + 1$ are irreducible over $\mathbb{F}_2$. If they were not irreducible, they would have a root, as there are degree 3, and it is easy to check that neither 0 nor 1 are roots. Hence, they are both irreducible, and K and L are fields.
2. In both K and L, $1, x, x^2$ forms a basis over $\mathbb{F}_2$, and so there are $2^3 = 8$ elements.
3. Let $y = x + 1$. I claim that if $x^3 + x^2 + 1 = y^3 + y + 1 = 0$. And this is easy to check

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

Hence the ring homomorphism

$$\begin{aligned} \mathbb{F}_2[x] &\to \mathbb{F}_2[y] \\ x &\mapsto y - 1 \end{aligned}$$

takes the ideal $(x^3 + x^2 + 1)$ to the ideal $(y^3 + y + 1)$. Hence, this induces a homomorphism of the quotient rings $K \to L$. This is a field homomorphism, and is therefore an injective map between two sets of the same cardinality. It is therefore a bijection and hence an isomorphism.

Exercise 4 *More splitting fields*

Let $f(x) \in K[x]$ be a polynomial of degree n, and let L/K be its splitting field. Show that

$$[L : K] \leq n!$$

Solution 4

We proceed by induction on the degree of $f(x)$. Clearly this is true if $f(x)$ is linear. Otherwise, we can consider the field $K_1 = K[x]/(f(x))$. Denoting by α the image of x in this field, we have that

$$f(x) = (x - \alpha) f_1(x)$$

in $K_1[x]$. The splitting field of $f(x)$ over K will be the splitting field of $f_1(x)$ over K_1, which, by induction has degree at most

$$[L : K_1] \leq (\deg f_1)! = (n - 1)!$$

as $\deg f_1 = n - 1$. Furthermore, as $\deg f = n$, we have that

$$[K_1 : K] \leq n$$

Thus

$$[L : K] = [L : K_1][K_1 : K] \leq (n - 1)! \times n = n!$$

Exercise 5 *Complexity*

Let $f(x) = x^3 + x + 1 \in \mathbb{Q}[x]$. You may assume freely that this is irreducible, and let K be the field $\mathbb{Q}[x]/(f(x))$

1. Is $K/\mathbb{Q}$ a separable extension? Why?
2. Is $K/\mathbb{Q}$ a normal extension? Why

   Hint: $f(x)$ is strictly increasing. Given any root $\alpha \in \mathbb{C}$, $K \cong \mathbb{Q}(\alpha)$. So?
3. Is $K/\mathbb{Q}$ a Galois extension? Why?

Solution 5

1. Yes, as we are working over a field of characteristic 0.
2. No. $f(x)$ is strictly increasing over $\mathbb{R}$, which implies it has exactly 1 real root. Hence K is isomorphic to a subfield of $\mathbb{R}$, which cannot contain the complex roots of $f(x)$. Thus $f(x)$ doesn't split in K, and so K is not normal.
3. No, as every Galois extension is normal and K is not

Exercise 6 *The real Galois group*

Determine $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ (by which I mean tell me what group it is isomorphic to).

Solution 6

As $\mathbb{C} = \mathbb{R}(i)$, any $\mathbb{R}$-automorphism of $\mathbb{C}$ is entirely determined by where i is mapped to. We must map i to another root of its minimal polynomial $x^2 + 1$, so either

$$i \mapsto i \quad \text{or} \quad i \mapsto -i$$

The first of these is the identity map, while the second satisfies $\varphi(\varphi(a+bi)) = a + bi$, and so squares to the identity. Thus $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.