MAU34106 - Galois Theory

Practice Sheet 1

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 *Irreducible polynomials of low degree*

1. Let K be a field. Show that a polynomial of degree 2 or 3 is irreducible in $K[x]$ if and only if does not have a root in K.
2. Pick a field K and give an example of a degree 4 polynomial that is not irreducible, but does not have a root in K.
3. Show that $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$.
4. Show that $x^2 + 1$ is irreducible in $\mathbb{F}_3[x]$.
5. Show that $x^3 - 2x - 2$ is irreducible in $\mathbb{Q}[x]$

   Hint: Recall Gauss' Lemma: a polynomial with integer coefficients is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$

Solution 1

1. If a polynomial $f(x)$ of degree greater than 1 has a root $a \in K$, then $f(x) = (x-a)g(x)$, so $f(x)$ is not irreducible. If $f(x)$ is not irreducible, then $f(x) = g(x)h(x)$ for some non-constant $g(x), h(x) \in K[x]$ with

$$\deg(f) = \deg(g) + \deg(h)$$

In particular, if $\deg(f) = 2$, then we must have $\deg(g) = \deg(h) = 1$, as they are both non-zero integers. If $\deg(f) = 3$ then one of $\deg(g), \deg(h)$ is 1 and the other is 2. In either case, $f(x)$ has a linear factor $(x - a) \in K[x]$ for some $a \in K$, and so

$$f(a) = (a - a)h(a) = 0.$$

2. Lets take $K = \mathbb{Q}$. We know that $x^2 + 1$ has no roots in $\mathbb{Q}$, so the polynomial

$$f(x) = (x^2 + 1)^2 = x^4 + 2x^2 + 1$$

is a reducible polynomial of degree 4, which has no roots in $\mathbb{Q}$.

3. As it is degree 2, it suffices to show that it has no roots in $\mathbb{F}_2$:

$$0^2 + 0 + 1 = 1 \neq 0, \quad 1^2 + 1 + 1 = 1 \neq 0$$

Hence, the polynomial is irreducible.

4. As it is degree 2, it suffices to check that it has no roots in $\mathbb{F}_3$:

$$0^2 + 1 = 1 \neq 0, \quad 1^2 + 1 = 2 = -1 \neq 0, \quad (-1)^2 + 1 = 2 = -1 \neq 0.$$

Hence, the polynomial is irreducible.

5. As it is degree 3, it is reducible if and only if it has a root in $\mathbb{Q}$. By Gauss' Lemma, it suffices to check for roots in $\mathbb{Z}$. Any such root must divide the constant term, so we just need to check ± 1, ± 2. Letting

$$f(x) = x^3 - 2x - 2$$

we see that

$$f(-2) = -6, \ f(-1) = -1, \ f(1) = -3, \ f(2) = 2$$

and so $f(x)$ is irreducible.

Exercise 2 *Factorisation in finite fields*

Recall the finite field of order 2 $\mathbb{F}_2 = \{0, 1\}$. Write down every polynomial of degree exactly 4 as a product of irreducibles.

Remark: Although we will not present this method in the solution, it is arguably faster to write down every irreducible polynomial of degree at most 3*, and consider all possible products of these of degree* 4*. All polynomials not in this list of products will be irreducible*

Solution 2

As mentioned in the remark, actually factorising the polynomials is the worst way to go about this. We will show a couple of examples of how it can be done though, just for sake of illustration

There are 16 such polynomials. They factorise as follows:

$$\begin{aligned}
x^4 &= x^4,\\
x^4 + 1 &= (x+1)^4,\\
x^4 + x &= x(x+1)(x^2+x+1),\\
x^4 + x^2 &= x^2(x+1)^2,\\
x^4 + x^3 &= x^3(x+1),\\
x^4 + x + 1 &= x^4 + x + 1,\\
x^4 + x^2 + 1 &= (x^2+x+1)^2,\\
x^4 + x^3 + 1 &= x^4 + x^3 + 1,\\
x^4 + x^2 + x &= x(x^3+x+1),\\
x^4 + x^3 + x &= x(x^3+x^2+1),\\
x^4 + x^3 + x^2 &= x^2(x^2+x+1),\\
x^4 + x^2 + x + 1 &= (x+1)(x^3+x^2+1),\\
x^4 + x^3 + x + 1 &= (x+1)^2(x^2+x+1),\\
x^4 + x^3 + x^2 + 1 &= (x+1)(x^3+x+1),\\
x^4 + x^3 + x^2 + x &= x(x+1)^3,\\
x^4 + x^3 + x^2 + x + 1 &= x^4 + x^3 + x^2 + x + 1.
\end{aligned}$$

We'll look at three of these computations in detail: 1 is a root of $x^4 + x^2 + x + 1$, and so it is divisible by $(x-1) = (x+1)$. Thus, we must have

$$x^4+x^2+x+1 = (x+1)(x^3+ax^2+bx+1) = x^4+(a+1)x^3+(a+b)x^2+(b+1)x+1.$$

Comparing coefficients, we can check

$$a+1=0,\ a+b=1,\ b+1=1$$

which implies

$$a=-1=1,\ b=0.$$

Finally, we check that x^3+x^2+1 has no roots in $\mathbb{F}_2$, and is therefore irreducible.

For x^4+x^2+1, we know it cannot have a linear factor, as it does not have a root. If it has a quadratic factor, then there exist $a,b,c,d\in\mathbb{F}_2$ such that

$$x^4+x^2+1=(x^2+ax+b)(x^2+cx+d)=x^4+(a+c)x^3+(b+d+ac)x^2+(ad+bc)x+bd.$$

Comparing coefficients, we must have that

$$b=d=1,\ a=c,\ ac=1,\ a=c=1.$$

Finally, to see that $x^4+x^3+x^2+x+1$ is irreducible, we note that it has no roots in $\mathbb{F}_2$ and hence no linear factors. If it has a quadratic factor, then, as in the last case, we can find $a,b,c,d,\in\mathbb{F}_2$ such that

$$a+c=1,\ b+d+ac=1,\ ad+bd=1,\ bd=1.$$

The last equality implies $b=d=1$. $a+c=1$ implies one of a or c is 0, and hence $ac=0$. But then $b+d+ac=1+1+0=0\neq 1$. So no such quadratic factors can exist.

The others can be worked out similarly, but honestly, just work out the irreducibles in lower degree and consider their products.

Exercise 3 *Square roots and simple extensions*

1. Let K be a field of characteristic other than 2 and let L be an extension of degree 2. Show that $L=K(\sqrt{\alpha})$ for some $\alpha\in K$.

   Hint: Pick a K-basis $\{1,\beta\}$ of L, and note that the quadratic formula

   $$ax^2+bx+c\quad\Rightarrow x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

   works in any field of characteristic other than 2.

2. We say that $c \in K$ is a square if there exists $d \in K$ such that $c = d^2$. Choose non-zero $a, b \in K$, and pick square roots $\sqrt{a}, \sqrt{b}$ in some field extension of K. Show that $K(\sqrt{a}) = K(\sqrt{b})$ if and only if $\frac{a}{b}$ is a square in K.

Solution 3

1. We pick a basis $1, \beta$ of L over K. Since $\dim_K(L) = 2$, we must have that $\{1, \beta, \beta^2\}$ is a linearly dependent set, and so there exist $a, b, c \in K$, not all 0 such that

$$a\beta^2 + b\beta + c = 0.$$

Furthermore, we can assume $a \neq 0$, as β and 1 are linearly independent. Thus β is a root of

$$ax^2 + bx + c$$

and so

$$\beta = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Without loss of generality, we assume it is the positive square root. Let $\alpha = b^2 - 4ac$. Then $\sqrt{\alpha} = 2a\beta + b \in L$ is an element of L. It suffices to show that we can write every element of L in the form $A + B\sqrt{\alpha}$ for some $A, B \in K$.

Take an element $C + D\beta \in L$, where $C, D \in K$. This is equal to

$$C + D\beta = \left(C - \frac{Db}{2a}\right) + \frac{D}{2a}\sqrt{\alpha}$$

and so taking $A = \left(C - \frac{Db}{2a}\right)$ and $B = \frac{D}{2a}$ gives the result.

2. If $K(\sqrt{a}) = K(\sqrt{b}) = K$, then both square roots are in K. Hence both a and b are squares in K, and so $\frac{a}{b}$ is a square in K.

If $K(\sqrt{a}) = K(\sqrt{b}) \neq K$, then neither square root is in K. Since the fields are equal, there exist $\alpha, \beta \in K$ such that

$$\sqrt{a} = \alpha + \beta\sqrt{b}.$$

As $\sqrt{a} \notin K$, we must have $\beta \neq 0$.

Squaring both sides, we get

$$a = (\alpha^2 + b\beta^2) + 2\alpha\beta\sqrt{b}$$

Since $\{1, \sqrt{a}\}$ is a basis, we must have

$$\alpha^2 + b\beta^2 = a, \quad 2\alpha\beta = 0.$$

Since $\beta \neq 0$, and K has characteristic different to 2, this implies that $\alpha = 0$ and so

$$a = b\beta^2 \quad \Rightarrow \quad \frac{a}{b} = \beta^2.$$

So $\frac{a}{b}$ is a square in K.

Conversely, if $\frac{a}{b} = \beta^2$ is a square in K, then $a = \beta^2 b$ and and $\sqrt{a} = \pm\sqrt{b}$, which clearly generates the same field extension as $\sqrt{b}$.

Exercise 4 *Degree calculations and minimal polynomials*

1. Show that
$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$$
2. Show that
$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6}) : \mathbb{Q}] < 8$$
3. Determine the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$. Be sure to justify minimality.

Solution 4

1. It is easy to check, either by direct inspection and Gauss' lemma, or by Eisenstein's criterion, that $x^2 - 2$ is irreducible over $\mathbb{Q}$ and is therefore the minimal polynomial of $\sqrt{2}$. This implies that
$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.$$
If we can show that $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$, then tower law implies that
$$\begin{aligned}[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : Q] &= [\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}] \\ &= [\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2} : \mathbb{Q}] = 4\end{aligned}$$

Unfortunately, we cannot just apply Eisenstein's criterion. We will have to show x^2-3 is irreducible directly. Suppose it is not irreducible. Then $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ and so

$$\sqrt{3} = a + b\sqrt{2}$$

with $a, b \in \mathbb{Q}$, $b \neq 0$ (as $\sqrt{3}$ is irrational). Squaring both sides we find

$$3 = a^2 + 2b^2 + 2ab\sqrt{2}.$$

We must have $a = 0$, as $\{1, \sqrt{2}\}$ are a basis over $\mathbb{Q}$, and so there must exist $b \in \mathbb{Q}$ such that

$$3 = 2b^2.$$

The argument is then concluded by giving your favourite proof of the irrationality of $\sqrt{\frac{3}{2}}$. My choice today is to note that, by letting $b = \frac{r}{s}$ for some integers $r, s \in \mathbb{Z}$, we have that

$$3s^2 = 2r^2.$$

The power of 2 in the prime factorisation of the left hand side is even, while the power of 2 on the right hand side is odd. This is impossible, so no such b can exist.

2. Note that $\sqrt{6} = \sqrt{2}\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and so

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

is of degree $4 < 8$.

3. We give two approaches. The first involves computing a polynomial with $\sqrt{2} + \sqrt{3}$ via resultants

$$C(x) = \mathrm{Res}_y(y^2 - 2, (y-x)^2 - 3) = \det \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & -2x & 1 \\ -2 & 0 & x^2 - 3 & -2x \\ 0 & -2 & 0 & x^2 - 3 \end{pmatrix}$$

which we can compute to be

$$C(x) = x^4 - 10x^2 + 1$$

I claim this is irreducible. By Gauss' lemma, if it has a rational root, it has an integer root, which must divide 1. Checking $x = \pm 1$, we see neither of these are roots.

So suppose we can factorise it into quadratics:

$$\begin{aligned} x^4 - 10x^2 + 1 &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a+c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd \end{aligned}$$

Comparing coefficients, we must have

$$a + c = 0,\ b + d + ac = -10,\ ad + bc = 0,\ bd = 1$$

By Gauss Lemma, we have $a, b, c, d \in \mathbb{Z}$, so $b = d = \pm 1$. From this, as $a = -c$, we must have that

$$-a^2 = ac = -10 - b - d = \begin{cases} -12 \text{ if } b = 1 \\ -8 \text{ if } b = -1 \end{cases}$$

Neither of these have integer solutions, so no such factorisation exists. Thus, the minimal polynomial of $\sqrt{2} + \sqrt{3}$ is $x^4 - 10x^2 + 1$.

Alternatively, we can try the method of optimism and squaring: Let $x = \sqrt{2} + \sqrt{3}$. Then

$$x^2 = 2 + 3 + 2\sqrt{6} = 5 + 2\sqrt{6}.$$

Therefore

$$(x^2 - 5)^2 = (4\sqrt{6})^2 = 24$$

and so

$$x^4 - 10x^2 + 1 = 0.$$

This gives that $\sqrt{2} + \sqrt{3}$ is a root of $x^4 - 10x^2 + 1$, which we have previously shown to be irreducible. This means that it is the minimal polynomial.

Remark 1. *This is an example of an irreducible polynomial to which we cannot apply Eisenstein's criterion, even with a shift in variable!*

Exercise 5 *Classified*

Using the results of Exercise 3, classify all degree 2 extensions of $\mathbb{R}$.

Solution 5

From Exercise 3, every quadratic extension is of the form $\mathbb{R}(\sqrt{a})$ for some non-zero non-square $a \in \mathbb{R}$ (i.e. $a < 0$), and

$$\mathbb{R}(\sqrt{a}) = \mathbb{R}(\sqrt{b})$$

if and only if $\frac{a}{b}$ is a square (i.e. non-negative/positive since $a \neq 0$). This means two quadratic extensions $\mathbb{R}(\sqrt{a})$ and $\mathbb{R}(\sqrt{b})$ are equal if $\frac{a}{b} > 0$. This occurs if and only if a and b have the same sign. As such, every negative number a gives the same extension. Thus, there is a unique quadratic extension of $\mathbb{R}$ given by $\mathbb{R}(\sqrt{-1})$.

Exercise 6 *Eisenstein won't help you here*

Show that $f(x) = x^{105} - 9$ is irreducible over $\mathbb{Z}$.

Hint: The roots of $f(x)$ are $\sqrt[105]{9}e^{\frac{2\pi ik}{105}}$ for $k = 0, 1, \ldots, 104$. Suppose we can factorise $f(x) = g(x)h(x)$ into polynomials with integer coefficients. What must those coefficients look like?

Solution 6

Suppose we can factorise $f(x) = g(x)h(x)$ into a product of polynomials of degrees $\deg(g), \deg(h)$, $\deg(g) + \deg(h) = 105$. Exactly one of these degrees must be even. Without loss of generality, take it to be $\deg(g)$. The constant coefficient of g, up to a sign, is the product of all the roots of $g(x)$. Each of these roots is of the form $\sqrt[105]{9}e^{\frac{2\pi ik}{105}}$ for some k, and so has absolute value $\sqrt[105]{9}$. Therefore the constant coefficient of $g(x)$ is

$$9^{\frac{2\ell}{105}} = 3^{\frac{4\ell}{105}}$$

for some $\ell > 0$, with

$$2\ell = \deg(g) < 105$$

This can only be an integer if $\frac{4\ell}{105}$ is an integer, which requires that $105|\ell$. But $0 < \ell < 105$, so no such ℓ exists. Thus, $g(x)$ cannot have integer coefficients.

Exercise 7 *Hungry for power?*

Consider the first three symmetric power sums in $\mathbb{Q}[x_1, x_2, x_3]$:

$$\begin{aligned} h_1(x_1, x_2, x_3) &= x_1 + x_2 + x_3, \\ h_2(x_1, x_2, x_3) &= x_1^2 + x_2^2 + x_3^2, \\ h_3(x_1, x_2, x_3) &= x_1^3 + x_2^3 + x_3^3. \end{aligned}$$

1. Write h_1, h_2, h_3 in terms of the elementary symmetric polynomials

$$\begin{aligned} e_1(x_1, x_2, x_3) &= x_1 + x_2 + x_3, \\ e_2(x_1, x_2, x_3) &= x_1x_2 + x_1x_3 + x_2x_3, \\ e_3(x_1, x_2, x_3) &= x_1x_2x_3. \end{aligned}$$

2. Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of

$$x^3 - 6x^2 + 21x + 15.$$

   Determine $\alpha_1^3 + \alpha_2^3 + \alpha_3^3$.

3. Determine a polynomial

$$x^3 + ax^2 + bx + c$$

   with roots $\beta_1, \beta_2, \beta_3$ such that

$$\begin{aligned} \beta_1 + \beta_2 + \beta_3 &= 2, \\ \beta_1^2 + \beta_2^2 + \beta_3^2 &= 42, \\ \beta_1^3 + \beta_2^3 + \beta_3^3 &= 62. \end{aligned}$$

   Hint: Try writing e_k in terms of h_ℓ.

4. Hence or otherwise solve

$$\begin{aligned} \beta_1 + \beta_2 + \beta_3 &= 2, \\ \beta_1^2 + \beta_2^2 + \beta_3^2 &= 42, \\ \beta_1^3 + \beta_2^3 + \beta_3^3 &= 62. \end{aligned}$$

Solution 7

1. The easy one is $h_1 = e_1$. The second power sum h_2 is degree 2, so it is a linear combination of

$$e_1^2 = x_1^2 + x_2^+ x_3^2 + 2(x_1x_2 + x_1x_3 + x_2x_3)$$

and e_2. Comparing coefficients, it is easy to see

$$h_2 = e_1^2 - 2e_2.$$

Similarly, h_3 must be a linear combination of e_1^3, e_1e_2 and e_3. Expanding these out and comparing coefficients, we find

$$h_3 = e_1^3 - 3e_1e_2 + 3e_3$$

2. This is

$$h_3(\alpha_1, \alpha_3, \alpha_3) = e_1^3 - 3e_1e_2 + 3e_3.$$

From the Vieta formulas, we know that

$$e_1 = 6,\ e_2 = 21,\ e_3 = -15$$

so

$$h_3 = 216 - 378 - 45 = -207.$$

3. We have that $e_1 = h_1$, and

$$h_2 = e_1^2 - 2e_2 = h_1^2 - 2e_2 \quad \Rightarrow \quad e_2 = \frac{1}{2}(h_1^2 - h_2).$$

Similarly, we find

$$e_3 = \frac{1}{6}h_1^3 - \frac{1}{2}h_1h_2 + \frac{1}{3}h_3.$$

Evaluating these on $\beta_1, \beta_2, \beta_3$, we therefore have

$$e_1 = 2,\ e_2 = -19,\ e_3 = -20$$

which means, via the Vieta formulas, that $\beta_1, \beta_2, \beta_3$ are the roots of

$$x^3 - 2x^2 - 19x + 20.$$

4. We know that $\beta_1, \beta_2, \beta_3$ are roots of

$$x^3 - 2x^2 - 19x + 20.$$

which we know can be solved in radicals, but we can try and find a rational root. It is not too hard to see that $x = 1$ is a root, and so we compute

$$x^3 - 2x^2 - 19x + 20 = (x - 1)(x^2 - x - 20) = (x - 1)(x + 4)(x - 5).$$

Thus, up to reordering

$$\beta_1 = 1,\ \beta_2 = -4,\ \beta_3 = 5.$$