Peize Liu
St. Peter's College
University of Oxford

Problem Sheet 2

B3.1: Galois Theory

A Brilliant work!
Basically no problems.

3 November, 2020

In these problems K denotes an arbitrary field, $K[x]$ denotes the ring of polynomials in one variable x over K and $K(x)$ the ring of rational functions in the variable x (i.e. the fraction field of $K[x]$). If p is a prime number, then $\mathbb{F}_p$ denotes the field of integers modulo p. Recall the multiplicative group of $\mathbb{F}_p$ is cyclic.

Question 1

Let K be a finite field. Show that there exists a positive integer d and a prime number p such that $|K| = p^d$.

Hint: what is the prime subfield of K?

Proof. This is a standard Part A Rings & Modules question.

If $\operatorname{char} K = 0$, then $m1_F \neq (n1_F)^{-1}$ for $m, n \in \mathbb{Z}\backslash\{0\}$. It follows that

$$\{(m1_F)(n1_F)^{-1} \in F : \ m \in \mathbb{Z}, n \in \mathbb{Z}\backslash\{0\}\} = \mathbb{Q} \subseteq K$$

In particular K is not finite. Hence $\operatorname{char} K = p$ for some prime $p > 0$. Then

$$\{0_F, 1_F, 1_F + 1_F, \cdots, (p-1)1_F\} = \mathbb{F}_p \subseteq K$$

Since K is finite, K is a finite-dimensional vector space over $\mathbb{F}_p$. Hence $K \cong \mathbb{F}_p^d$ for some $n \in \mathbb{N}$. Then $|K| = p^d$. ✓ □

Nice

A

Question 2

Factorise $f(x) = x^6 + x^3 + 1$ into irreducible factors over K for each of $K = \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_{19}, \mathbb{Q}$.

Calculate the formal derivative Df. Over which of these fields K do the irreducible factors of f have distinct roots in any splitting field for f?

Proof.

- First we factorise f over $\mathbb{C}$:

  Let $t = x^3$. Then

  $$x^6 + x^3 + 1 = 0 \implies t^2 + t + 1 = 0 \implies t_{1,2} = \frac{-1 \pm \sqrt{3}\mathrm{i}}{2} = \mathrm{e}^{\pm\frac{2\pi}{3}\mathrm{i}} \implies x^3 = \mathrm{e}^{\pm\frac{2\pi}{3}\mathrm{i}}$$

  The all 6 roots are

  $$x_1 = \mathrm{e}^{\frac{2\pi}{9}\mathrm{i}},\ x_2 = \mathrm{e}^{\frac{4\pi}{9}\mathrm{i}},\ x_3 = \mathrm{e}^{\frac{8\pi}{9}\mathrm{i}},\ x_4 = \mathrm{e}^{\frac{10\pi}{9}\mathrm{i}}, x_5 = \mathrm{e}^{\frac{14\pi}{9}\mathrm{i}},\ x_6 = \mathrm{e}^{\frac{16\pi}{9}\mathrm{i}}$$

  Hence $f(x) = (x^3 - \mathrm{e}^{\frac{2\pi}{3}\mathrm{i}})(x^3 - \mathrm{e}^{-\frac{2\pi}{3}\mathrm{i}}) = (x - \mathrm{e}^{\frac{2\pi}{9}\mathrm{i}})(x - \mathrm{e}^{\frac{4\pi}{9}\mathrm{i}})(x - \mathrm{e}^{\frac{8\pi}{9}\mathrm{i}})(x - \mathrm{e}^{\frac{10\pi}{9}\mathrm{i}})(x - \mathrm{e}^{\frac{14\pi}{9}\mathrm{i}})(x - \mathrm{e}^{\frac{16\pi}{9}\mathrm{i}}) \in \mathbb{C}[x]$.

- Consider $f \in \mathbb{Q}[x]$. Let $p(x) = f(x+1)$. Then f is irreducible over $\mathbb{Q}$ if and only if p is irreducible over $\mathbb{Q}$. But

  $$p(x) = (x+1)^6 + (x+1)^3 + 1 = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3$$

  is irreducible over $\mathbb{Q}$ be Eisenstein's criterion with $p = 3$. Hence f is irreducible over $\mathbb{Q}$. ✓

- Consider $f \in \mathbb{F}_3[x]$. We note that $p(x) = f(x+1) = x^6$ in $\mathbb{F}_3[x]$. Then $f(x) = p(x-1) = (x-1)^6$ in $\mathbb{F}_3[x]$. ✓

- Consider $f \in \mathbb{F}_2[x]$. We factorise f by brute force:

  The irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$ is $x^2 + x + 1$. The irreducible polynomial of degree 3 in $\mathbb{F}_2[x]$ are $x^3 + x + 1$ and $x^3 + x^2 + 1$. By division algorithm:

  $$f(x) = (x^2 + x + 1)(x^4 + x^3) + 1$$
  $$f(x) = (x^3 + x + 1)^2 + 1$$
  $$f(x) = (x^3 + x^2 + 1)^2 + 1$$

  Then f has no factor of degree 2 and 3. It is clear that f has no roots in $\mathbb{F}_2$. We deduce that f is irreducible over $\mathbb{F}_2$. ✓

- Consider $f \in \mathbb{F}_{19}[x]$. First we analyse the structure of the multiplicative group $\mathbb{F}_{19}^\times$. We have the group isomorphism $\mathbb{F}_{19}^\times \cong \mathbb{Z}/18\mathbb{Z}$. We observe that $2 \in \mathbb{F}_{19}^\times$ is a generator of $\mathbb{F}_{19}^\times$:

  $$2^1 = 2 \qquad 2^2 = 4 \qquad 2^3 = 8 \qquad 2^4 = -3 \qquad 2^5 = -6 \qquad 2^6 = 7 \qquad 2^7 = -5 \qquad 2^8 = 9 \qquad 2^9 = -1$$

$$2^{10} = -2 \qquad 2^{11} = -4 \qquad 2^{12} = -8 \qquad 2^{13} = 3 \qquad 2^{14} = 6 \qquad 2^{15} = -7 \qquad 2^{16} = 5 \qquad 2^{17} = -9 \qquad 2^{18} = 1$$

So 2 has order 18 in $\mathbb{F}_{19}^{\times}$. It is a generator. In addition from the list above we can read out the elements of order 9 in $\mathbb{F}_{19}^{\times}$: 4, -3, 9, -2, 6, 5 and the elements of order 3: 7 and -8.

Let $t = x^3$. Then $t^2 + t + 1 = 0$ implies that t is a third root of unity, which is a order 3 element in $\mathbb{F}_{19}^{\times}$. Hence $t_1 = 7$, $t_2 = -8$. We have $f(x) = (x^3 - 7)(x^3 + 8)$. It is clear that the set of roots of $x^3 - 7 = 0$ or $x^3 + 8 = 0$ is exactly the set of order 9 elements in $\mathbb{F}_{19}^{\times}$. We deduce that

$$f(x) = (x-4)(x+3)(x-9)(x+2)(x-6)(x-5)$$ ✓

- Now we consider the problem that if f is separable over $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_{19}$ or $\mathbb{Q}$.

  We have factorise f into distinct linear factors on $\mathbb{F}_{19}$. So $f \in \mathbb{F}_{19}[x]$ is separable.

  Over the splitting field of $\mathbb{Q}$, f is factorised into distinct linear factors. So $f \in \mathbb{Q}[x]$ is separable.

  f is factorised into non-distinct linear factors in $\mathbb{F}_3[x]$. So $f \in \mathbb{F}_3[x]$ is not separable.

  The only remaining case is $f \in \mathbb{F}_2[x]$. The formal derivative $Df(x) = 6x^5 + 3x^2 = x^2 \in \mathbb{F}_2[x]$. The unique root of Df in any extension field of $\mathbb{F}_2[x]$ is $x = 0$, which is not a root of f in any extension field of $\mathbb{F}_2[x]$. Hence f has simple roots only in the splitting field of f. So f is separable. ✓ Great A □

Question 3

Show that if f is a polynomial of degree n over K, then its splitting field has degree less than or equal to $n!$ over K.

Proof. In fact this also serves as an existence lemma of splitting fields.

We use induction on $\deg f$. Base case: If $\deg f = 1$, $f(x) = ax + b$ splits over K. Then $F = K$ is the splitting field of K and $[F : K] = 1$.

Induction case: Suppose that the result holds for $\deg f < n$. Suppose that $f \in K[x]$ has degree n and does not split over K. Let g be an irreducible factor of f ($\deg g > 1$). There exists a simple extension $K \subseteq K(u)$ such that g is the minimal polynomial of u on K. Then $[K(u) : K] = \deg g$. $f(x) = (x - u)h(x)$ for some $h \in K[x]$. As $\deg h < n$, by induction hypothesis, there exists a splitting field F of h over $K(u)$. Hence F is a splitting field of f over K. By Tower Law:

$$[F : K] = [F : K(u)][K(u) : K] \leqslant (n-1)! \cdot \deg g \leqslant n!$$ ✓ Very concise A

which completes the induction. □

Question 4

Find the degrees of the splitting fields of the following polynomials.

(a) $x^3 - 1$ over $\mathbb{Q}$

(b) $x^3 - 2$ over $\mathbb{Q}$

(c) $x^5 - t$ over $\mathbb{F}_{11}(t)$

Proof. (a) Let $\omega = \dfrac{-1 + \sqrt{3}\mathrm{i}}{2}$ be a root of $x^3 - 1 = 0$ over $\mathbb{C}$. Then

$$x^3 - 1 = (x-1)(x-\omega)(x-\omega^2) \in \mathbb{C}[x]$$

The splitting field of $x^3 - 1$ is $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{3}\mathrm{i})$. Since the minimal polynomial of $\sqrt{3}\mathrm{i}$ is $x^2 + 3$ over $\mathbb{Q}$, we have $[\mathbb{Q}(\sqrt{3}\mathrm{i}) : \mathbb{Q}] = 2$. We deduce that the degree of splitting field of $x^3 - 1$ over $\mathbb{Q}$ is 2. ✓

(b) We have

$$x^3 - 2 = (x - 2^{1/3})(x - 2^{1/3}\omega)(x - 2^{1/3}\omega^2) \in \mathbb{C}[x]$$

The splitting field of x^3-2 is $\mathbb{Q}(2^{1/3},\omega)=\mathbb{Q}(2^{1/3},\sqrt{3}\mathrm{i})$. Since x^3-2 is the minimal polynomial of $2^{1/3}$ over $\mathbb{Q}$, $[\mathbb{Q}(2^{1/3}):\mathbb{Q}]=3$. Since $\sqrt{3}\mathrm{i}\notin\mathbb{R}\supseteq\mathbb{Q}(2^{1/3})$, x^2+3 is the minimal polynomial of $\sqrt{3}\mathrm{i}$ over $\mathbb{Q}(2^{1/3})$. Hence $[\mathbb{Q}(2^{1/3},\sqrt{3}\mathrm{i}):\mathbb{Q}(2^{1/3})]=2$. Finally by tower law,

$$[\mathbb{Q}(2^{1/3},\sqrt{3}\mathrm{i}):\mathbb{Q}]=[\mathbb{Q}(2^{1/3},\sqrt{3}\mathrm{i}):\mathbb{Q}(2^{1/3})][\mathbb{Q}(2^{1/3}):\mathbb{Q}]=6$$

We deduce that the degree of splitting field of x^3-2 over $\mathbb{Q}$ is 6.

(c) Note that $\mathbb{F}_{11}(t)$ is a field so it is a UFD. By applying Eisenstein criterion [1] with the the prime $p=t$, we deduce that x^5-t is irreducible in $\mathbb{F}_{11}(t)[x]$. On the splitting field of x^5-t, we have

Think you mean since $\mathbb{F}_{11}[t]$ is a UFD

$$x^5-t=(x-t^{1/5})(x-t^{1/5}\zeta)(x-t^{1/5}\zeta^2)(x-t^{1/5}\zeta^3)(x-t^{1/5}\zeta^4)$$

where ζ is the primitive fifth root of unity. We note that $\mathbb{F}_{11}^{\times}\cong\mathbb{Z}/10\mathbb{Z}$ has elements of order 5. Then $\zeta\in\mathbb{F}_{11}\subseteq\mathbb{F}_{11}(t)$. So the splitting field of x^5-t over $\mathbb{F}_{11}(t)$ is $\mathbb{F}_{11}(t)(t^{1/5})$. x^5-t is the minimal polynomial of $t^{1/5}$. We conclude that $[\mathbb{F}_{11}(t)(t^{1/5}):\mathbb{F}_{11}(t)]=5$.

Good work A^-

□

Question 5

Let $L=\mathbb{Q}\left(2^{1/3},3^{1/4}\right)$. Compute the degree of L over $\mathbb{Q}$.

Proof. x^3-2 is the minimal polynomial of $2^{1/3}$ over $\mathbb{Q}$ (by Eisenstein's criterion it is irreducible). So $[\mathbb{Q}(2^{1/3}):\mathbb{Q}]=3$. x^4-3 is the minimal polynomial of $3^{1/4}$ over $\mathbb{Q}$ (by Eisenstein's criterion it is irreducible). So $[\mathbb{Q}(3^{1/4}):\mathbb{Q}]=4$. By tower law, we know that

$$[\mathbb{Q}(2^{1/3},3^{1/4}):\mathbb{Q}]=4[\mathbb{Q}(2^{1/3},3^{1/4}):\mathbb{Q}(3^{1/4})]=3[\mathbb{Q}(2^{1/3},3^{1/4}):\mathbb{Q}(2^{1/3})]$$

In particular, 12 divides $[\mathbb{Q}(2^{1/3},3^{1/4}):\mathbb{Q}]$.

On the other hand, since x^3-2 annihilates $2^{1/3}$ over $\mathbb{Q}\subseteq\mathbb{Q}(3^{1/4})$, we have $[\mathbb{Q}(2^{1/3},3^{1/4}):\mathbb{Q}(3^{1/4})]\leqslant 3$. So $[\mathbb{Q}(2^{1/3},3^{1/4}):\mathbb{Q}]\leqslant 12$.

We conclude that $[\mathbb{Q}(2^{1/3},3^{1/4}):\mathbb{Q}]=12$. Perfect! A

□

Question 6

Recall that $\alpha\in\mathbb{C}$ is algebraic over $\mathbb{Q}$ if α satisfies a (monic) polynomial over $\mathbb{Q}$, equivalently if $[\mathbb{Q}(\alpha):\mathbb{Q}]<\infty$. Let $\mathbb{A}=\{\alpha\in\mathbb{C}:\alpha$ is algebraic over $\mathbb{Q}\}$

(a) Show that $\mathbb{A}$ is the union of all the subfields L of $\mathbb{C}$ which are finite extensions of $\mathbb{Q}$

(b) Prove that $\mathbb{A}$ is a subfield of $\mathbb{C}$. [Hint: if $\alpha,\beta\in\mathbb{A}$, consider the extension $\mathbb{Q}(\alpha,\beta):\mathbb{Q}\cdot$]

(c) Prove that $\mathbb{A}:\mathbb{Q}$ is not a finite extension.

Proof. This is a standard Part A Rings & Modules question. (In fact this is exactly Question 1 in Sheet 3 of Part A Rings & Modules.)

(a) Suppose that $L|\mathbb{Q}$ is a finite extension. Then it is algebraic. So every element in L is algebraic over $\mathbb{Q}$. Hence $L\subseteq\mathbb{A}$. On the other hand, for $\alpha\in\mathbb{A}$, α is algebraic over $\mathbb{Q}$. So $\mathbb{Q}(\alpha)|\mathbb{Q}$ is a finite extension with degree equal to the degree of minimal polynomial of α over $\mathbb{A}$. Then we deduce that

$$\mathbb{A}=\bigcup\{L\subseteq\mathbb{Q}:\ L|\mathbb{Q}\text{ is finite}\}$$

(b) First it is clear that $0,1\in\mathbb{A}$. For $\alpha,\beta\in\mathbb{A}$, by tower law we have $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]=[\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]\leqslant\deg m_\alpha\cdot\deg m_\beta$. So $\mathbb{Q}(\alpha,\beta)|\mathbb{Q}$ is finite and hence algebraic. Then $\alpha\pm\beta$, $\alpha\beta$ and α/β $(\beta\neq 0)$ are all in $\mathbb{Q}(\alpha,\beta)$ and hence in $\mathbb{A}$. We then deduce that $\mathbb{A}$ is a subfield of $\mathbb{Q}$.

(c) Suppose that $[\mathbb{A}:\mathbb{Q}]=k$ is finite. Take $n>k$. Note that by Eisenstein's criterion $x^n-2\in\mathbb{Q}[x]$ is irreducible for $n\geqslant 2$. Let $\alpha\in\mathbb{A}$ be a root of $x^n-2\in\mathbb{A}[x]$. Then we know that x^n-2 is the minimal polynomial of α over $\mathbb{Q}$. This implies that

[1] The version of Eisenstein's criterion that I use here is: Suppose that R is a unique factorization domain. Let $f(x)=\sum_{i=0}^{n}a_ix^i\in R[x]$ be a non-constant primitive polynomial. If there exists a prime $p\in R$ such that $p\nmid a_n$, $p\mid a_0,a_1,\ldots,a_{n-1}$, and $p^2\nmid a_0$, then f is irreducible in $R[x]$.

$[\mathbb{A}:\mathbb{Q}] \geqslant [\mathbb{Q}(\alpha):\mathbb{Q}] = n > k$, which is a contradiction. Therefore $\mathbb{A}$ is not a finite extension of $\mathbb{Q}$. ✓ □

Great A

Question 7

Which of the following fields are normal extensions of $\mathbb{Q}$?

1. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$
2. $\mathbb{Q}\left(2^{1/4}\right)$
3. $\mathbb{Q}(\alpha)$, where $\alpha^4 - 10\alpha^2 + 1 = 0$

Proof.

1. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $(x^2-2)(x^2-3)$ over $\mathbb{Q}$. By Theorem 3.16, $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ is a normal extension. ✓
2. $\mathbb{Q}\left(2^{1/4}\right)|\mathbb{Q}$ is not a normal extension. The minimal polynomial of $2^{1/4}$ over $\mathbb{Q}$ is x^4-2 (by Eisenstein's criterion it is irreducible). But
$$x^4-2 = (x-2^{1/4})(x+2^{1/4})(x-2^{1/4}\mathrm{i})(x+2^{1/4}\mathrm{i}) \in \mathbb{C}[x]$$
and $2^{1/4}\mathrm{i} \notin \mathbb{R} \supseteq \mathbb{Q}\left(2^{1/4}\right)$. By definition $\mathbb{Q}\left(2^{1/4}\right)|\mathbb{Q}$ is not normal. ✓
3. $\mathbb{Q}(\alpha)|\mathbb{Q}$ is normal. Here is a method by brute force.

   First we solve $\alpha^4 - 10\alpha^2 + 1 = 0$ in $\mathbb{C}$:
$$\alpha^4 - 10\alpha^2 + 1 = 0 \implies (\alpha^2-5)^2 = 24 \implies \alpha^2 = 5 \pm 2\sqrt{6} \implies \alpha = \pm\sqrt{5 \pm 2\sqrt{6}} = \pm\left(\sqrt{2} \pm \sqrt{3}\right)$$
   We claim that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We show this in the case that $\alpha = \sqrt{2}+\sqrt{3}$. The other cases are similar.

   One direction is clear: $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) \implies \mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Conversely, we observe that
$$(\sqrt{2}+\sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3}$$
   Then we have
$$\sqrt{2} = \frac{1}{2}\left((\sqrt{2}+\sqrt{3})^3 - 9(\sqrt{2}+\sqrt{3})\right) \in \mathbb{Q}(\sqrt{2}+\sqrt{3}) \qquad \sqrt{3} = \frac{1}{2}\left(11(\sqrt{2}+\sqrt{3}) - (\sqrt{2}+\sqrt{3})^3\right) \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$$
   Hence $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$. We deduce that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

   From the first part we have shown that $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ is normal. Hence $\mathbb{Q}(\alpha)|\mathbb{Q}$ is normal. ✓ □

Nice method

A