MA3D5 Galois Theory
Sheet 2 Solutions

Peize Liu

22 Oct 2024

Section A: Warn-up questions

Exercise 2.1

Let $\alpha = \sqrt{-5} \in \mathbb{C}$ and consider the field $K = \mathbb{Q}(\alpha) \subseteq \mathbb{C}$. Express

$$\frac{1 + 2\alpha + 3\alpha^2 + 4\alpha^3}{5 + 7\alpha + 11\alpha^2} \in K$$

in the form $a + b\alpha$ with $a, b \in \mathbb{Q}$.

Using that $\alpha^2 = -5$,

$$\frac{1 + 2\alpha + 3\alpha^2 + 4\alpha^3}{5 + 7\alpha + 11\alpha^2} = \frac{-14 - 18\alpha}{-50 + 7\alpha} = \frac{(-14 - 18\alpha)(50 + 7\alpha)}{(-50 + 7\alpha)(50 + 7\alpha)} = \frac{-70 - 998\alpha}{-2745} = \frac{14}{549} + \frac{998}{2745}\alpha.$$

Exercise 2.2

Let $f \in \mathbb{R}[x]$. If $z \in \mathbb{C}$ is a root of f, show that $\overline{z}$ is another root of f. (Bear in mind that $f(z)$ is just some complex number, so $\overline{f(z)}$ makes sense. Recall that complex conjugation is a ring homomorphism, so that $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ and $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$.)

Since complex conjugation is an $\mathbb{R}$-algebra homomorphism, $f(\overline{z}) = \overline{f(z)}$. Since z is a root of f, then $f(z) = 0$. So $f(\overline{z}) = \overline{f(z)} = 0$. So $\overline{z}$ is another root of f.

Exercise 2.3

Show that any polynomial $f \in \mathbb{R}[x]$ factorises as $f = c h_1 h_2 \cdots h_s$, where $c \in \mathbb{R}$ and each $h_i \in \mathbb{R}[x]$ is either a monic linear polynomial $h_i = x - a_i$ or a monic quadratic polynomial $h_i = x^2 + b_i x + c_i$ with $b_i^2 - 4c_i < 0$.

By fundamental theorem of algebra, f splits into linear factors over $\mathbb{C}$: $f(x) = c(x - z_1) \cdots (x - z_n)$ for some $z_1, ..., z_n \in \mathbb{C}$. For each root z_i of f, if $z_i \notin \mathbb{R}$, then $\overline{z}_i$ is also a root of f by Question 2. So $\overline{z}_i = z_j$ for some $j \neq i$. In other words, the imaginary roots of f comes in pairs. So we can write $f \in \mathbb{C}[x]$ as

$$f(x) = c(x - x_1) \cdots (x - x_r)(x - y_1)(x - \overline{y}_1) \cdots (x - y_s)(x - \overline{y}_s)$$

where $x_1, ..., x_r \in \mathbb{R}$ and $y_1, ..., y_s \in \mathbb{C} \setminus \mathbb{R}$. Note that $(x - y_i)(x - \overline{y}_i) = x^2 - 2\,\mathrm{Re}(y_i)x + |y_i|^2$. The discriminant corresponding to this quadric $\Delta_i < 0$ because it has no real roots. In summary, we have $f \in \mathbb{R}[x]$ factoring over $\mathbb{R}$ as

$$f(x) = c(x - x_1) \cdots (x - x_r)(x^2 - 2\,\mathrm{Re}(y_1)x + |y_1|^2) \cdots (x^2 - 2\,\mathrm{Re}(y_s)x + |y_s|^2).$$

Exercise 2.4

Consider the ($\mathbb{R}$-algebra) homomorphism $\varphi : \mathbb{R}[x] \to \mathbb{C}$ determined by $\varphi(x) = i$. Check that $\varphi\left(x^2+1\right) = 0$. Show that $\ker\varphi$ is the ideal $\left(x^2+1\right)$ generated by x^2+1. [If $p \in \ker\varphi$, then consider division with remainder of p by x^2+1.]

Recall that $f = x^3 - 2 \in \mathbb{Q}[x]$ is irreducible. (Easy to prove this case: if $f = gh$, then one of g and h must be linear, so f has a root in $\mathbb{Q}$, contradiction.)

Let $\alpha = \sqrt[3]{2} \in \mathbb{R}$. Consider $\varphi : \mathbb{R}[x] \to \mathbb{C}$ determined by $\varphi(x) = \alpha$. Check that $\varphi(f) = 0$. Show that $\ker\varphi$ is the ideal (f) generated by f.

The only $\mathbb{R}$-algebra homomorphism $\varphi\colon \mathbb{R}[x] \to C$ with $\varphi(x) = \mathrm{i}$ is given by $f(x) \longmapsto f(\mathrm{i})$. So $\varphi(x^2+1) = \mathrm{i}^2+1 = 0$. Hence $\left\langle x^2+1\right\rangle \subseteq \ker\varphi$. To show the reverse inclusion, suppose that $g(x) \in \ker\varphi$. By division algorithm, $g(x) = (x^2+1)h(x) + (ax+b)$ for some $a, b \in \mathbb{R}$ It follows that

$$0 = \varphi(g) = \varphi(x^2+1)\varphi(h) + a\mathrm{i} + b = a\mathrm{i} + b.$$

Hence $a = b = 0$. So $g(x) = (x^2+1)h(x) \in \left\langle x^2+1\right\rangle$. We conclude that $\ker\varphi = \left\langle x^2+1\right\rangle$.

Since $\alpha = \sqrt[3]{2}$, $\alpha^3 = 2$. Then $\varphi(f) = \varphi(x^3-2) = \alpha^3 - 2 = 0$. Since $\mathbb{R}[x]$ is a PID (this could be proved using division algorithm), $\ker\varphi = \langle g\rangle$ for some $g \in \mathbb{R}[x]$. Since $f \in \ker\varphi(x)$, $f = gh$ for some $h \in \mathbb{R}[x]$. But f is irreducible, so h is a unit (i.e. $h \in \mathbb{R}^\times$). It follows that $\ker\varphi = \langle g\rangle = \langle f\rangle$.

Section B: Problems to hand in

Exercise 2.5

Let $\omega \in \mathbb{C}$ be a primitive 5 th root of unity, so $\omega^5 = 1, \omega \neq 1\big)$.

(a) Show that $\omega^4 + \omega^3 + \omega^2 + \omega + 1 = 0$.

(b) Show that $\omega \notin \mathbb{R}$. (Hint: Analysis.)

(c) Show that $\mathbb{Q}(\omega) = \mathbb{Q}\left(\omega^i\right), i = 1, 2, 3, 4$.

(a) This follows from the fact that $0 = \omega^5 - 1 = (\omega - 1)(\omega^4 + \omega^3 + \omega^2 + \omega + 1)$ and that $\omega - 1 \neq 0$.

(b) Consider the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^5 - 1$. Its derivative $f'(x) = 5x^4$ satisfies $f'(x) \geqslant 0$ for all $x \in \mathbb{R}$. Hence f is non-decreasing. If $\omega \in \mathbb{R}$, that $f(\omega) = 0$ implies that $f(x)$ is identically zero between 1 and ω. Since $\omega \neq 1$ and f is a polynomial, this is impossible.

(c) That $\mathbb{Q}\left(\omega^i\right) \subseteq \mathbb{Q}(\omega)$ is obvious. As $\gcd(i, 5) = 1$ for $i = 1, 2, 3, 4$, there exists $k_i \in \{1, 2, 3, 4\}$ such that $ik_i = 1 \bmod 5$ and thus $\omega^{ik_i} = \omega, i = 1, 2, 3, 4$. This shows the other direction.

Exercise 2.6

(a) Show that there does not exist an element $\alpha \in \mathbb{R}$, such that $\alpha^2 = -1$.

(b) Show that for all $D < 0, D \in \mathbb{R}$, $[\mathbb{R}(\sqrt{D}) : \mathbb{R}] = 2$.

(a) It is a very standard exercise in Analysis I showing that $x^2 \geqslant 0$ for all x in an ordered field from the axioms.

- Suppose that $x > 0$. By the axiom $x^2 = x \cdot x \geqslant 0$.
- Suppose that $x = 0$. Then $x^2 = 0 \geqslant 0$.
- Suppose that $x < 0$. $x + (-x) = 0 > x$ implies that $-x > 0$. Then $x^2 = (-x) \cdot (-x) \geqslant 0$.

(b) (b) The polynomial $x^2 + D$ is irreducible in $\mathbb{R}[x]$, because otherwise it would have a root in $\mathbb{R}$, which we showed in (a) to be impossible. The field $\mathbb{R}(\sqrt{D}) = \left\{ \frac{a+b\sqrt{D}}{c+d\sqrt{D}}; a, b, c, d \in \mathbb{R}, (c,d) \neq (0,0) \right\}$. However we can clear the denominator of $\frac{a+b\sqrt{D}}{c+d\sqrt{D}}$ by multiplying by $c - d\sqrt{D}$. This shows that $\{1, \sqrt{D}\}$ is a basis for $\mathbb{R}[\sqrt{D}]$.

Exercise 2.7

Let $f(X) = X^5 - 2$.

(a) Show that f is irreducible.

(b) Show that f has a real root.

(c) Show that there are three roots α, β, γ of f, such that $\mathbb{Q}(\alpha), \mathbb{Q}(\beta), \mathbb{Q}(\gamma)$ are three pairwise distinct fields. You may assume that for all roots of α of f, $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leqslant 5$.

1. Apply the Eisenstein criterion with the prime 2.

2. The real continuous function $f(x) = x^5 - 2$ satisfies $f(-1) = -3 < 0$ and $f(2) = 30 > 0$. By the intermediate value theorem we deduce that f has a real root.

3. Take α to be a real root of f. Then for any other root $\beta \neq \alpha$ of f, $\omega = \beta/\alpha \neq 1$, satisfies $\omega^5 = 1$. From Q5(b), we know that ω is not real. We can also check that $\beta_k = \alpha\omega^k, k = 0, 1, 2, 3, 4$ are distinct roots of f. Since suppose we would have $0 \leqslant i < j \leqslant 4$ such that $\beta_i = \beta_j$,this would imply that $\beta_j/\beta_i = \omega^{j-i} = 1$. Since $\gcd(j-i, 5) = 1$, there exists $k \in \{1, 2, 3, 4\}$ such that $k(j-i) \equiv 1 \bmod 5$. Hence $\omega = \omega^{(j-i)k} = 1$. This contradicts that $\omega \notin \mathbb{R}$.

   Now suppose that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta_k)$ for some $k \in \{1, 2, 3, 4\}$. Then $\omega^k = \beta^k/\alpha \in \mathbb{Q}(\alpha)$ but we know that ω^k is not real as it satisfies the conditions of Q5. Contradiction.

   Now suppose that $\mathbb{Q}(\beta_2) = \mathbb{Q}(\beta_1)$. Then $\beta_1^2/\beta_2 = \alpha \in \mathbb{Q}(\beta_1)$. So $\mathbb{Q}(\alpha)$ is a subfield of $\mathbb{Q}(\beta_1)$ and because $[\mathbb{Q}(\beta_1) : \mathbb{Q}] \leqslant 5$ it follows from the tower law that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta_1)$. This in turn implies that $\beta_1 \in \mathbb{R}$ and hence $\omega \in \mathbb{R}$. A contradiction to Q5(b).

   In conclusion, $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\alpha\omega)$ and $\mathbb{Q}(\alpha\omega^2)$ are three pairwise distinct fields.

Exercise 2.8

Let $f = x^3 + x + 2 \in \mathbb{C}[x]$.

(a) Express the roots of f in terms of radicals of rational numbers.

(b) What is the smallest subfield of $\mathbb{C}$ that contains all the roots of f ? (Express your answer in the form $\mathbb{Q}(\alpha)$ for some specified $\alpha \in \mathbb{C}$.)

(a) Observe that -1 is a root of f. Then

$$f(x) = x^3 + x + 2 = (x+1)(x^2 - x + 2) = (x+1)\left(x - \frac{1+\sqrt{-7}}{2}\right)\left(x - \frac{1-\sqrt{-7}}{2}\right).$$

Hence the roots of f are -1, $\frac{1+\sqrt{7}\mathrm{i}}{2}$, and $\frac{1-\sqrt{7}\mathrm{i}}{2}$.

(b) The field is $\mathbb{Q}(\sqrt{-7})$.

Section C: Additional problems

Exercise 2.9

If K is a field (or even an integral domain) prove that $K[x]$ is an integral domain.

Consider non-zero $f, g \in K[x]$ such that $fg = 0$. Write $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$, where $a_n \neq 0$ and $b_m \neq 0$. Note that

$$f(x)g(x) = \left(\sum_{i=0}^{k} a_i x^i\right)\left(\sum_{i=0}^{m} b_i x^i\right) = a_n b_m x^{n+m} + \sum_{i=0}^{n+m-1} c_i x^i.$$

Since K is an integral domain, $a_n b_m \neq 0$. Hence $fg \neq 0$. We conclude that $K[x]$ is an integral domain.

Exercise 2.10

Consider a cubic $f = x^3 + px + q$ with $p, q \in \mathbb{C}$. Let $\alpha_1, \alpha_2, \alpha_3$ be the 3 roots (in $\mathbb{C}$, possibly with repeats). Define the discriminant Δ to be

$$\Delta = (\alpha_1 - \alpha_2)^2 (\alpha_1 - \alpha_3)^2 (\alpha_2 - \alpha_3)^2$$

Comparing coefficients after expanding $f = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$, express Δ in terms of p and q. (The answer should be $-27q^2 - 4p^3$. You can certainly do this by hand, but it might be easier to use a computer to do the multiplications.)

Besides a brute force computation, we can also use the following trick. Let $S_n = S(\alpha_1, \alpha_2, \alpha_3)$ be the n-th elementary symmetric polynomial in $\alpha_1, \alpha_2, \alpha_3$. Then we know that

$$S_1 = \alpha_1 + \alpha_2 + \alpha_3 = 0; \qquad S_2 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = p; \qquad S_3 = \alpha_1\alpha_2\alpha_3 = -q.$$

Note that $\Delta = (\alpha_1 - \alpha_2)^2 (\alpha_1 - \alpha_3)^2 (\alpha_2 - \alpha_3)^2$ is a symmetric polynomial in $\alpha_1, \alpha_2, \alpha_3$ and is homogeneous of degree 6. By the *fundamental theorem of symmetric polynomials*, Δ is a polynomial in $\mathbb{Z}[S_1, S_2, S_3]$. Since $S_1 = 0$, by comparing the degree we have $\Delta = aS_3^2 + bS_2^3 = aq^2 + bp^3$ for some $a, b \in \mathbb{Z}$. To determine a, b we consider the following two special cases:

- $\alpha_1 = \alpha_2 = t$ and $\alpha_3 = -2t$. In this case we have $\Delta = 0$, $q = -2t^3$, and $p = -3t^2$. Hence $4a + 27b = 0$.
- $\alpha_1 = t$, $\alpha_2 = -t$ and $\alpha_3 = 0$. In this case we have $\Delta = 4t^6$, $q = 0$, and $p = -t^2$. Hence $4 = -b$.

Solving the equations we obtain that $a = -27$ and $b = -4$. That is, $\Delta = -27q^2 - 4p^3$.

Exercise 2.11

What is the degree of the extension $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$, where α is a root of $x^5 - 3x^3 - 2x^2 + 6$? (Beware: not every polynomial is irreducible ... in which case it might depend on which root we're talking about ...)

In $\mathbb{C}[x]$ we have

$$x^5 - 3x^3 - 2x^2 + 6 = (x^3 - 2)(x^2 - 3) = (x + \sqrt{3})(x - \sqrt{3})(x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega)(x - \sqrt[3]{2}\omega^2)$$

where ω is a primitive third root of unity.

If $\alpha = \sqrt{3}$ or $-\sqrt{3}$, then $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3})$ is a quadratic extension of $\mathbb{Q}$. If $\alpha = \sqrt[3]{2}$, $\sqrt[3]{2}\omega$ or $\sqrt[3]{2}\omega^2$, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ since the minimal polynomial of α over $\mathbb{Q}$ is given by $x^3 - 2$.