MA3D5 Galois Theory
Sheet 1 Solutions

Peize Liu

9 Oct 2024

These exercises are not assessed. There will be solutions much later, but better to solve them first and discuss them with one another and/or the TAs before that. They relate to Chapter 1. Some may be new to you, but can all be treated using elementary methods you know, often "division with remainder".

Recall: If $L \subseteq \mathbb{C}$ is a subfield of $\mathbb{C}$ and $\alpha \in \mathbb{C}$, then $L(\alpha)$ denotes the smallest subfield of $\mathbb{C}$ that contains L and α : equivalently

$$L(\alpha) = \left\{ \left. \frac{p(\alpha)}{q(\alpha)} \right| p, q \in L[x] \text{ and } q(\alpha) \neq 0 \right\}$$

Similarly $L(\alpha_1, \alpha_2, \ldots, \alpha_s)$ is the field of all rational combinations of all of the α_i and elements of L. (You can say $L(\alpha_1, \alpha_2) = (L(\alpha_1))(\alpha_2)$ or $L(\alpha_1, \alpha_2) = (L(\alpha_2))(\alpha_1)$ if you prefer adjoining elements one at a time.)

If you already took Algebraic Number Theory, then that's cheating and you must explain the solutions to anybody who asks who did not.

Exercise 1.1

Let $\alpha = \sqrt{7}$ (the positive root, by convention) and $K = \mathbb{Q}(\alpha) \subseteq \mathbb{R}$.

(a) Recall that $\alpha \notin \mathbb{Q}$. (This was in Foundations. We don't need the proof of this every time, but good to be able to say correctly that this is true.)

(b) Show that if $p \in \mathbb{Q}[x]$ is a polynomial (with rational coefficients), then $p(\alpha) \in K$ is the same as $a + b\alpha$ for some $a, b \in \mathbb{Q}$.

(c) If $a, b \in \mathbb{Q}$ are not both zero, show that $1/(a + b\alpha) = c + d\alpha$ for some $c, d \in \mathbb{Q}$.

(d) Show that

$$K = \{a + b\alpha \mid a, b \in \mathbb{Q}\}$$

(e) Find a $\mathbb{Q}$-basis of K and deduce that $\dim_{\mathbb{Q}} K = 2$.

1. Suppose that $\alpha \in \mathbb{Q}$. Then there exists $p, q \in \mathbb{Z}$ such that $\gcd(p, q) = 1$ and $\alpha = p/q$. Squaring both sides gives $7q^2 = p^2$. Hence $7 \mid p^2$. Since 7 is square-free, $7 \mid p$. So $7^2 \mid p^2$. It follows that $7 \mid q^2$ and hence $7 \mid q$, contradicting that p and q are coprime. Hence $\alpha \notin \mathbb{Q}$.

2. Write $p(x) = \sum_{i=0}^{n} c_i x^i$ for $c_i \in \mathbb{Q}$. For $i = 2k$, $\alpha^i = (\alpha^2)^k = 7^k \in \mathbb{Q}$; for $i = 2k + 1$, $\alpha^i = (\alpha^2)^k \cdot \alpha = 7^k \alpha$. It follows that $p(\alpha) = \sum_{k=0}^{\lfloor n/2 \rfloor} c_{2k} 7^k + \left(\sum_{k=0}^{\lfloor (n-1)/2 \rfloor} c_{2k+1} 7^k \right) \alpha = a + b\alpha$ for some $a, b \in \mathbb{Q}$.

3. $$\frac{1}{a + b\alpha} = \frac{a - b\alpha}{(a + b\alpha)(a - b\alpha)} = \frac{a - b\alpha}{a^2 - b^2\alpha^2} = \frac{a}{a^2 - 7b^2} + \frac{-b}{a^2 - 7b^2}\alpha.$$

4. For any $\dfrac{p(\alpha)}{q(\alpha)} \in K$, by (c) we have $1/q(\alpha) = c + d\alpha$ for some $c, d \in \mathbb{Q}$. Now by (b) we have

$$\frac{p(\alpha)}{q(\alpha)} = p(\alpha)(c + d\alpha) = a + b\alpha$$

for some $a, b \in \mathbb{Q}$.

5. We claim that $\{1, \alpha\}$ is a $\mathbb{Q}$-basis of K. Suppose that $a+b\alpha = 0$ for some $a, b \in \mathbb{Q}$. If $b \neq 0$ then $\alpha = -a/b \in \mathbb{Q}$ which contradicts (a). Hence $a = b = 0$. So $1, \alpha$ are linearly independent over $\mathbb{Q}$. Moreover, (d) shows that $\{1, \alpha\}$ spans K. Hence it is a $\mathbb{Q}$-basis. We have $\dim_{\mathbb{Q}} K = 2$.

Exercise 1.2

Show that if $\alpha = \sqrt{d}$ for some nonzero $d \in \mathbb{Q}$, then $\mathbb{Q}(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Q}\}$ and compute $\dim_{\mathbb{Q}}$. (You might consider the case where $d = e^2$ is a square, $e \in \mathbb{Q}$, separately.) For which such d is $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R}$?

Write $d = e^2 a$ for some $e \in \mathbb{Q}_{\geqslant 0}$ and $a \in \mathbb{Z}$ square-free (not having any square divisor). If $a = 1$, then $\alpha = e$, and $\mathbb{Q}(\alpha) = \mathbb{Q}$. So $\dim_{\mathbb{Q}} \mathbb{Q}(\alpha) = 1$. If $a \neq 1$, then $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{e^2 a}) = \mathbb{Q}(\sqrt{a})$. There are two cases:

1. $a > 0$. Then $\alpha \in \mathbb{R}$ and hence $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. The same proof as Question 1 shows that $\mathbb{Q}(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Q}\}$ and hence $\dim_{\mathbb{Q}} \mathbb{Q}(\alpha) = 2$.

2. $a < 0$. Then $\alpha \notin \mathbb{R}$ and hence $\mathbb{Q}(\alpha) \not\subseteq \mathbb{R}$. Note that for 1.(a) we immediately obtain that $\alpha \notin \mathbb{Q}$ as $\mathbb{Q} \subseteq \mathbb{R}$. For 1.(b)–(e), the same proof still works. $\dim_{\mathbb{Q}} \mathbb{Q}(\alpha) = 2$.

Exercise 1.3

Let $\alpha = \sqrt{2}, \beta = \sqrt{3}$. Recall that $\alpha \notin \mathbb{Q}$ and $\beta \notin \mathbb{Q}$.

Show that $\alpha \notin \mathbb{Q}(\beta)$. (In other words, by the question above, show that there must be something wrong if you try to write $\alpha = a + b\beta$ with $a, b \in \mathbb{Q}$.)

Is $\beta \in \mathbb{Q}(\alpha)$? Considering the sequence of $\mathbb{Q}$-vector spaces

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \beta)$$

prove that $\dim_{\mathbb{Q}} \mathbb{Q}(\alpha, \beta) > 2$. Let $\gamma = \sqrt{6}$. Is $\gamma \in \mathbb{Q}(\alpha)$? Is $\gamma \in \mathbb{Q}(\beta)$? Is $\alpha \in \mathbb{Q}(\gamma)$? Is $\beta \in \mathbb{Q}(\gamma)$? (No, no, no, no, no, no, no ... just as the first one above.)

Why is $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha, \beta)$? Use the dimension considerations above to show that these fields are not equal.

Find a quadratic polynomial $f = x^2 + ax + b \in \mathbb{Q}[x]$ (i.e. $a, b \in \mathbb{Q}$) so that $f(\alpha\beta) = 0$. Find another polynomial $g \in \mathbb{Q}[x]$ so that $g(\alpha+\beta) = 0$(g is not necessarily quadratic). [Hint: in principle, when looking for a polynomial $g \in \mathbb{Q}[x]$ with γ as a root, you can start computing a few of $\gamma, \gamma^2, \gamma^3, \ldots$ and look for linear $\mathbb{Q}$-linear relations among them. Later you'll know you may need to go up to deg = 4 here.]

Suppose that $\alpha \in \mathbb{Q}(\beta)$. Then $\sqrt{2} = a + b\sqrt{3}$ for some $a, b \in \mathbb{Q}$. Squaring both sides gives $2 = a^2 + 3b^2 + 2ab\sqrt{3}$, or $\sqrt{3} = \dfrac{2 - a^2 - 3b^2}{2ab} \in \mathbb{Q}$, which is a contradiction. Hence $\alpha \notin \mathbb{Q}(\beta)$.

The same proof shows that $\beta \notin \mathbb{Q}(\alpha)$. In particular, $\mathbb{Q}(\alpha) \subsetneq \mathbb{Q}(\alpha, \beta)$. Hence $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] > 1$. By tower law,

$$\dim_{\mathbb{Q}} \mathbb{Q}(\alpha, \beta) = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] > [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2.$$

We have $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha, \beta)$ because $\mathbb{Q} \subseteq \mathbb{Q}(\alpha, \beta)$ and $\gamma = \alpha\beta \in \mathbb{Q}(\alpha, \beta)$.

Note that $\dim_{\mathbb{Q}} \mathbb{Q}(\gamma) = 2 < \dim_{\mathbb{Q}} \mathbb{Q}(\alpha, \beta)$. So these two fields are not equal.

$\gamma = \alpha\beta = \sqrt{6}$. Squaring both sides gives $\gamma^2 = 6$. Hence $\gamma = \alpha\beta$ is a root of the polynomial $f(x) = x^2 - 6$. Let $\delta = \alpha + \beta = \sqrt{2} + \sqrt{3}$. Squaring both sides gives $\delta^2 = 5 + 2\sqrt{6}$. Hence $2\sqrt{6} = \delta^2 - 5$. Again squaring both sides gives $24 = \delta^4 - 10\delta^2 + 25$. Hence $\delta = \alpha + \beta$ is a root of the polynomial $g(x) = x^4 - 10x^2 + 1$.

Exercise 1.4

Show that $\mathbb{Q}\left(\alpha, \alpha\omega, \alpha\omega^2\right) = \mathbb{Q}(\alpha, \omega)$, where $\alpha = \sqrt[3]{2} \in \mathbb{R}$ and ω is any primitive cube root of unity. [Hint: to show $\mathbb{Q}\left(\alpha_1, \ldots\right) = \mathbb{Q}\left(\beta_1, \ldots\right)$, you just have to show that each $\alpha_i \in \mathbb{Q}\left(\beta_1, \ldots\right)$ and each $\beta_j \in \mathbb{Q}\left(\alpha_1, \ldots\right)$ - concretely, can you write α_i as a combination of the β_j 's, and conversely?]

Let $f = x^3 - 2$. Factorise f in $M[x]$ where $M = \mathbb{Q}(\alpha\omega)$. Compute an extension of M over which the irreducible quadratic factor splits (and so f splits too).

It is clear that $\mathbb{Q}\left(\alpha, \alpha\omega, \alpha\omega^2\right) \subseteq \mathbb{Q}(\alpha, \omega)$. For the reverse inclusion, we have $\alpha \in \mathbb{Q}\left(\alpha, \alpha\omega, \alpha\omega^2\right)$ and $\omega = \dfrac{\alpha\omega}{\alpha} \in \mathbb{Q}\left(\alpha, \alpha\omega, \alpha\omega^2\right)$. So the two fields are equal.

Write $\beta = \alpha\omega$. Note that $\beta^3 = 2$. Then

$$f(x) = x^3 - 2 = x^3 - \beta^3 = (x - \beta)(x^2 + \beta x + \beta^2) \in M[x].$$

We claim that the quadratic factor $x^2 + \beta x + \beta^2$ is irreducible in $M[x]$. Note that $x^2 + \beta x + \beta^2 = (x - \alpha)(x - \alpha\omega^2)$ in $\mathbb{C}[x]$. If it is reducible in $M[x]$, then $\alpha, \alpha\omega^2 \in M$. So $M = \mathbb{Q}(\alpha, \alpha\omega, \alpha\omega^2) = \mathbb{Q}(\alpha, \omega)$. Note that we have a non-trivial tower of extensions:

$$\mathbb{Q} \subsetneq \mathbb{Q}(\alpha) \subsetneq \mathbb{Q}(\alpha, \omega).$$

By tower law, $[M : \mathbb{Q}] = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \geqslant 4$. On the other hand, since $\beta^3 = 2$, in Question 6 we will check that $\left\{1, \beta, \beta^2\right\}$ is a $\mathbb{Q}$-basis of $M = \mathbb{Q}(\beta)$. Hence $[M : \mathbb{Q}] = 3$. This is a contradiction.

It follows that we have a non-trivial extension $\mathbb{Q}(\alpha, \omega) \mid \mathbb{Q}(\beta)$, and we have shown that f splits into linear factors in $\mathbb{Q}(\alpha, \omega)[x]$.

Exercise 1.5

Compute the following divisions with remainder. That is, for the following pairs $f, g \in K[x]$ compute polynomials

$$q, r \in K[x] \text{ with } \deg(r) < \deg(q) \text{ for which } f = qg + r$$

where, in truth, I only really care about r today, but you might happen to find q along the way.

(a) $f = x^n - 1, g = x - 1 \in \mathbb{Q}[x]$ for $n = 2, 3, 4, 5$.

(b) $f = 3x^5 + 7x^3 - 2x + 3, g = x^2 + 1 \in \mathbb{Q}[x]$. (Compare with the complex number $3i^5 + 7i^3 - 2i + 3$.)

(c) $f = x^3 - 5, g = x - \beta \in K[x]$ where $\beta = \sqrt[3]{5}$ and $K = \mathbb{Q}(\beta)$.

(a) $x^n - 1 = (x - 1)(x^{n-1} + \cdots + x + 1)$;

(b) $3x^5 + 7x^3 - 2x + 3 = (x^2 + 1)(3x^3 + 4x) + (-6x + 3)$. In terms of complex numbers (i is a root of $x^2 + 1$), this means $3^5 + 7^3 - 2 + 3 = -6 + 3$.

(c) $x^3 - 5 = x^3 - \beta^3 = (x - \beta)(x^2 + \beta x + \beta^2)$.

Exercise 1.6

Let $\alpha = \sqrt[3]{2}$ and $K = \mathbb{Q}(\alpha)$. Let $f = x^3 - 2 \in \mathbb{Q}[x]$ and note that $f(\alpha) = 0$.

(a) Show that $\alpha \notin \mathbb{Q}$. In particular, conclude that if $g = a + bx \in \mathbb{Q}[x]$ is a linear polynomial ($b \neq 0$), then $g(\alpha) \neq 0$.

(b) Suppose $g = a + bx + cx^2 \in \mathbb{Q}[x]$ is a quadratic polynomial ($c \neq 0$). Use the division algorithm to show that if $g(\alpha) = 0$ then g divides f (in $\mathbb{Q}[x]$). Conclude that $g(\alpha) \neq 0$ for all quadratic $g \in \mathbb{Q}[x]$.

(c) Use that to show that $\left\{1, \alpha, \alpha^2\right\}$ is a $\mathbb{Q}$-linearly independent subset of K.

(d) Show that if $\gamma = \sum_{i=0}^{n} a_i \alpha^i$, then γ is in the $\mathbb{Q}$-span of $\left\{1, \alpha, \alpha^2\right\}$. (In fact, this is a $\mathbb{Q}$-basis of K, as will become clear in a moment.)

(e) Solve $\left(a + b\alpha + c\alpha^2\right)(1+\alpha) \in \mathbb{Q}$ for $a, b, c \in \mathbb{Q}$. Use that to express $(1+\alpha)^{-1}$ as a $\mathbb{Q}$-linear combination of $\left\{1, \alpha, \alpha^2\right\}$.

(f) Express $(1 + 3\alpha)/\left(1 - \alpha^2\right)$ in the $\mathbb{Q}$-basis $\left\{1, \alpha, \alpha^2\right\}$ of K.

(a) This is the same as 1.(a). Suppose that $\alpha \in \mathbb{Q}$. Then there exists $p, q \in \mathbb{Z}$ such that $\gcd(p, q) = 1$ and $\alpha = p/q$. Squaring both sides gives $2q^3 = p^3$. Hence $2 \mid p^3$. Since 2 is cube-free, $2 \mid p$. So $2^3 \mid p^3$. It follows that $2^2 \mid q^3$ and hence $2 \mid q$, contradicting that p and q are coprime. Hence $\alpha \notin \mathbb{Q}$.

If $g(\alpha) = a + b\alpha = 0$, then $\alpha = -b/a \in \mathbb{Q}$, which is a contradiction. Hence α is not a root of any linear polynomial in $\mathbb{Q}[x]$.

(b) By division algorithm, $f = qg + r$ for some $q, r \in \mathbb{Q}[x]$ with $\deg r < \deg g = 2$. If $g(\alpha) = 0$, then we also have $r(\alpha) = 0$. But $r(x)$ is a constant or a linear polynomial. This contradicts (a).

(c) This is a rephrasing of (a) and (b).

(d) Write $k = \lfloor i/3 \rfloor$ to be the largest integer such that $3k \leqslant i$. Then we have $\alpha^i = (\alpha^3)^k \cdot \alpha^{i-3k} = 2^k \alpha^{i-3k} \in \operatorname{span}_{\mathbb{Q}} \left\{1, \alpha, \alpha^2\right\}$. It follows that $\gamma = \sum_{i=0}^{n} a_i \alpha^i \in \operatorname{span}_{\mathbb{Q}} \left\{1, \alpha, \alpha^2\right\}$.

(e) Note that $(1 - \alpha + \alpha^2)(1 - \alpha) = 1 + \alpha^3 = 3 \in \mathbb{Q}$. Hence

$$\frac{1}{1+\alpha} = \frac{(1 - \alpha + \alpha^2)}{(1 - \alpha + \alpha^2)(1 - \alpha)} = \frac{1}{3} - \frac{1}{3}\alpha + \frac{1}{3}\alpha^2.$$

(f) Similarly, $(1 + \alpha + \alpha^2)(1 - \alpha^2) = -3$. Hence

$$\frac{1 + 3\alpha}{1 - \alpha^2} = \frac{(1 + 3\alpha)(1 + \alpha + \alpha^2)}{(1 - \alpha^2)(1 + \alpha + \alpha^2)} = -\frac{1}{3}\left(7 + 5\alpha + 7\alpha^2\right).$$

Exercise 1.7

For each of $n = 1, 2, 3, 4, 5$, draw the nth roots of unity on the Argand diagram, and express them all in both polar and Cartesian coordinates. (You can find nice formulas in surds, either in memory or online or by trig, for the particular trig values you encounter, such as $\cos(2\pi/3)$ and similar.)

The n-th roots of unity are given by

$$\xi_n^k = \exp\left(\frac{2\pi k \mathrm{i}}{n}\right) = \cos\left(\frac{2\pi k}{n}\right) + \mathrm{i}\sin\left(\frac{2\pi k}{n}\right), \qquad k = 0, 1, \ldots, n-1.$$

- $n = 1$: 1.
- $n = 2$: $1, -1$.

- $n = 3$: $1, -\frac{1}{2} + \frac{\sqrt{3}}{2}\mathrm{i}, -\frac{1}{2} - \frac{\sqrt{3}}{2}\mathrm{i}$.
- $n = 4$: $1, \mathrm{i}, -1, -\mathrm{i}$.
- $n = 5$: $1, \frac{\sqrt{5}-1}{4} + \frac{\sqrt{10+2\sqrt{5}}}{4}\mathrm{i}, -\frac{\sqrt{5}+1}{4} + \frac{\sqrt{10-2\sqrt{5}}}{4}\mathrm{i}, -\frac{\sqrt{5}+1}{4} - \frac{\sqrt{10+2\sqrt{5}}}{4}\mathrm{i}, \frac{\sqrt{5}-1}{4} - \frac{\sqrt{10+2\sqrt{5}}}{4}\mathrm{i}$.

For $n = 5$, we have $\xi^5 - 1 = (\xi - 1)(\xi^4 + \xi^3 + \xi^2 + \xi + 1)$. So we need to compute the roots of $z^4 + z^3 + z^2 + z + 1$. Divide the whole equation by z^2 and completing the square, we have

$$\left(z + \frac{1}{z}\right)^2 + \left(z + \frac{1}{z}\right) - 1 = 0.$$

Hence $z + \frac{1}{z} = \frac{\pm\sqrt{5}-1}{2}$. Let $\xi := \exp\left(\frac{2\pi}{5}\right) = \cos\left(\frac{2\pi}{5}\right) + \mathrm{i}\sin\left(\frac{2\pi}{5}\right)$. Then this implies that

$$\xi + \frac{1}{\xi} = \xi + \xi^4 = \frac{\sqrt{5}-1}{2}; \qquad \xi^2 + \frac{1}{\xi^2} = \xi^2 + \xi^3 = -\frac{\sqrt{5}+1}{2}.$$

On the other hand,

$$\xi + \frac{1}{\xi} = \exp\left(\frac{2\pi}{5}\right) + \exp\left(-\frac{2\pi}{5}\right) = 2\cos\left(\frac{2\pi}{5}\right).$$

We deduce that $\cos\left(\frac{2\pi}{5}\right) = \frac{\sqrt{5}-1}{4}$ and hence $\sin\left(\frac{2\pi}{5}\right) = \sqrt{1 - \cos^2\left(\frac{2\pi}{5}\right)} = \frac{\sqrt{10+2\sqrt{5}}}{4}$.

Similarly for ξ^2 we have $\cos\left(\frac{4\pi}{5}\right) = -\frac{\sqrt{5}+1}{4}$ and $\sin\left(\frac{4\pi}{5}\right) = \sqrt{1 - \cos^2\left(\frac{4\pi}{5}\right)} = \frac{\sqrt{10-2\sqrt{5}}}{4}$.

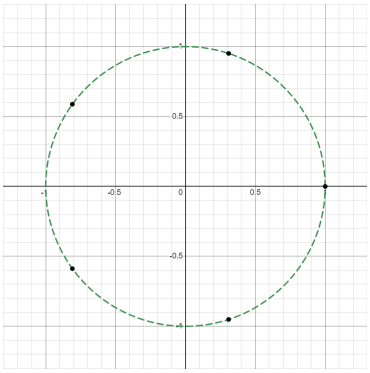

Figure 1: Fifth roots of unity

Exercise 1.8

Find the smallest subfield $L \subseteq \mathbb{C}$ over which the polynomial $x^5 - 5x^3 - x^2 + 5$ splits into linear factors. (Answer: $L = \mathbb{Q}(\sqrt{5}, \sqrt{-3})$.) Same for $\left(x^3 - 3\right)\left(x^2 + 3\right)$.

The subfield L of $\mathbb{C}$ is generated over $\mathbb{Q}$ by all the roots of the polynomial $x^5 - 5x^3 - x^2 + 5$, which factorises in $\mathbb{C}[x]$ as

$$x^5 - 5x^3 - x^2 + 5 = (x^2 - 5)(x^3 - 1) = (x + \sqrt{5})(x - \sqrt{5})(x - 1)(x - \omega)(x - \omega^2),$$

where ω is a primitive third root of unity. It follows that $L = \mathbb{Q}(\sqrt{5}, \omega) = \mathbb{Q}(\sqrt{5}, \sqrt{-3})$.

For $\left(x^3 - 3\right)\left(x^2 + 3\right)$, it factorises as

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

Hence $L = \mathbb{Q}(\sqrt[3]{3}, \omega, \sqrt{-3}) = \mathbb{Q}(\sqrt[3]{3}, \sqrt{-3})$. (Note that $\omega = \frac{-1+\sqrt{-3}}{2}$ lies in $\mathbb{Q}(\sqrt{-3})$.)