MA3D5 Galois Theory
Sheet 6 Solutions

Peize Liu

15 Nov 2024

Section A: Warn-up questions

Exercise 6.1

Recall that $\mathbb{F}_2 = \{0, 1\}$ is a finite field of 2 elements.

(a) Explain why $x^2 + x + 1 \in \mathbb{F}_2[x]$ is irreducible.

(b) Note that $\mathbb{F}_{2^2} = \mathbb{F}_2[x]/(x^2 + x + 1)$ is a finite field of $2^2 = 4$ elements: it is a field simply because the polynomial is irreducible, and it has a basis $1, \alpha$ as a vector space over $\mathbb{F}_2$. Denote by α the class of x in $\mathbb{F}_{2^2}$.

(c) Show that $\alpha(\alpha + 1) = 1$ (noting that $-1 = 1$ in $\mathbb{F}_2$). Conclude that $\alpha + 1$ is the multiplicative inverse of α.

(d) Draw the 4×4 addition and multiplication tables of $\mathbb{F}_{2^2}$.

(e) Show that the finite field $\mathbb{F}_{2^2}$ of 4 elements has no subfields other that itself and its prime subfield $\mathbb{F}_2$.

(a)–(d) are covered in my solution for Question 8 of Sheet 4. For (e), note that any subfield K of $\mathbb{F}_{2^2}$ is a $\mathbb{F}_2$-vector subspace of $\mathbb{F}_{2^2}$. Hence $|K| = |\mathbb{F}_2|^k$ for some $k \in Z_{>0}$. But $|K| \leqslant |\mathbb{F}_{2^2}| = 4$. We must have $k = 1$ or 2, corresponding to $K = \mathbb{F}_2$ or $K = \mathbb{F}_{2^2}$.

Exercise 6.2

Suppose L/K is an extension and $\alpha, \alpha' \in L$. Show that if $\alpha\alpha' \in K$ then $\alpha' \in K(\alpha)$ and moreover that $K(\alpha) = K(\alpha')$.

If $\alpha\alpha' = c \in K$, then $\alpha' = c\alpha^{-1} \in K(\alpha)$. Symmetrically $\alpha \in K(\alpha')$. Hence $K(\alpha) = K(\alpha')$.

Exercise 6.3

Compute all subgroups of the symmetric group S_3 and determine which are transitive.

Recall that a subgroup $H \leqslant S_n$ is called **transitive** if its natural action on the set $\{1, ..., n\}$ is transitive, i.e. for any $i, j \in \{1, ..., n\}$ there exists $\sigma \in H$ such that $\sigma(i) = j$. By orbit–stabiliser theorem, $|H| = |H \cdot x| \cdot |\operatorname{Stab}(x)|$. In particular, $n = |H \cdot x|$ divides $|H|$.

In the case of S_3, any transitive subgroup has order 3 or 6. These subgroups are $\langle(1\ 2\ 3)\rangle$ and S_3, and it is easy to check that they are indeed transitive.

Section B: Problems to hand in

Exercise 6.4

Let $f = x^{16} - x \in \mathbb{F}_2[x]$.

(a) Prove that f is separable over $\mathbb{F}_2$.

(b) Let $L/\mathbb{F}_2$ be a splitting field of f. How many elements does L have?

(c) Compute $[L : \mathbb{F}_2]$ (with justification).

(d) Show that there is an intermediate field M with $[M : \mathbb{F}_2] = 2$.

(e) Compute $[L : M]$ and justify it.

(a) By Lemma 9.26, f is separable if and only if f and its formal derivative $\mathrm{D}f$ are coprime in $K[x]$. For $f = x^{16} - x \in \mathbb{F}_2[x]$, we have

$$\mathrm{D}f = 16x^{15} - 1 = -1 \in \mathbb{F}_2[x]$$

as $16 = 0$ in $\mathbb{F}_2$. Clearly f and $\mathrm{D}f = -1$ are coprime, so f is separable.

(b) Let K be the set of roots of f in L. That is, $K = \{\alpha \in L \mid \alpha^{16} = \alpha\}$. We claim that K is a subfield of L. It is clear that $\alpha\beta^{-1} \in K$ for $\alpha \in K$ and $\beta \in K^\times$, so K is closed under multiplication and multiplicative inverse. For $\alpha, \beta \in K$, we have

$$(\alpha + \beta)^{16} = \alpha^{16} + \beta^{16} + \sum_{i=1}^{15} \binom{16}{i} \alpha^i \beta^{16-i} = \alpha^{16} + \beta^{16},$$

where we used the fact that 2 divides $\binom{16}{i}$ for $1 \leqslant i \leqslant 15$. Hence K is closed under addition. Moreover, $\alpha = -\alpha \in K$ since it has characteristic 2. We conclude that K is indeed a subfield of L.

We have the inclusions $\mathbb{F}_2 \subseteq K \subseteq L$, where K contains all roots of f. But L is a splitting field of f over $\mathbb{F}_2$, so we have $L = K$. Since f is separable, it has $\deg f = 16$ distinct roots in L. As L is exactly the set of roots of f, it has exactly 16 elements.

(c) Let $n = [L : \mathbb{F}_2]$. Then $L \cong \mathbb{F}_2^n$ as a $\mathbb{F}_2$-vector space. Then $16 = |L| = |\mathbb{F}_2|^n = 2^n$. Hence $n = 4$.

(d) Note that f can be factorised as

$$f(x) = x^{16} - x = x((x^3)^5 - 1) = x(x^3-1)(x^{15}+x^{12}+x^9+x^6+x^3+1) = x(x-1)(x^2+x+1)(x^{15}+x^{12}+x^9+x^6+x^3+1).$$

Then $x^2 + x + 1$ is a factor of f, and we have shown in Question 1.(a) that it is irreducible over $\mathbb{F}_2$. Let γ be a root of $x^2 + x + 1$. Then $M := \mathbb{F}_2(\gamma) \subseteq L$ has degree 2 over $\mathbb{F}_2$.

(e) By tower law, $[L : \mathbb{F}_2] = [L : M][M : \mathbb{F}_2]$. So $[L : M] = 2$.

Exercise 6.5

List and and justify the $n \in \{2, \ldots, 16\}$ for which there is a field with n elements. For each such field give a polynomial f such that it is the splitting field of this polynomial over its prime field.

Let K be a finite field. It contains a prime subfield $\mathbb{F}_p$ where $p = \operatorname{char} K$ is a prime number. Then K is a finite dimensional $\mathbb{F}_p$-vector space. If $\dim_{\mathbb{F}_p} K = [K : \mathbb{F}_p] = m$, then $|K| = |\mathbb{F}_p|^m = p^m$. We deduce that the cardinality of a finite field must be a power of prime. For $n \in \{2, ..., 16\}$, the prime powers are 2, 3, $4 = 2^2$, 5, 7, $8 = 2^3$, $9 = 3^2$, 11, 13, $16 = 2^4$.

Next, we shall construct a finite field of order p^n as a splitting field over $\mathbb{F}_p$ of some polynomial f. Following the previous question, the best candidate is $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. Let L be the splitting field over $\mathbb{F}_p$. The same argument as above shows that f is separable, and L is exactly the set of roots of f.[1] It follows that $|L| = \deg f = p^n$.

[1] When proving that the roots of f form a subfield of L, take care of the binomial coefficients — you need to show that p^n divides $\binom{p^n}{i}$ for $1 \leqslant i \leqslant p^n - 1$. See Question 2 of Sheet 7 for details.

Remark. We can prove moreover that the finite field of order p^n is unique up to isomorphism, as a result of the uniqueness of splitting field.

Let K be a finite field of order p^n. We know that $K^\times$ is a cyclic group of order $p^n - 1$. Hence any $\alpha \in K^\times$ satisfies $\alpha^{p^n-1} - 1 = 0$ and hence is a root of $f(x) := x^{p^n} - x \in \mathbb{F}_p[x]$. In addition, $0 \in K$ is also a root of f. Hence f splits over K and K is exactly the set of all roots of f. Hence K is the splitting field of f over $\mathbb{F}_p$. We conclude that $K \cong L$.

Exercise 6.6

Let $f = x^5 - 2$. Write down the splitting field of f over $\mathbb{Q}$ and compute its degree.

Let $\alpha := \sqrt[5]{2}$ be a real root of f, and ζ a primtive fifth root of unity. Then f is factorised over $\mathbb{C}$ as

$$f(x) = x^5 - 2 = (x-\alpha)(x-\alpha\zeta)(x-\alpha\zeta^2)(x-\alpha\zeta^3)(x-\alpha\zeta^4).$$

The splitting field of f over $\mathbb{Q}$ is given by $\mathbb{Q}(\alpha, \alpha\zeta, \alpha\zeta^2, \alpha\zeta^3, \alpha\zeta^4)$. It is clear that $K = \mathbb{Q}(\alpha, \zeta)$; on the other hand we have $\alpha \in K$ and $\zeta = \alpha\zeta/\alpha \in K$. Hence $K = \mathbb{Q}(\alpha, \zeta)$.

To compute the degree of K over $\mathbb{Q}$, consider the tower law:

$$[K : \mathbb{Q}] = [\mathbb{Q}(\alpha,\zeta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha,\zeta) : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}].$$

Since $x^5 - 2$ is the minimal polynomial of α over $\mathbb{Q}$, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$; since $x^4 + x^3 + x^2 + x + 1$ is the minimal polynomial of ζ over $\mathbb{Q}$, we have $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$. It follows that

$$[K : \mathbb{Q}] = 5[K : \mathbb{Q}(\alpha)] = 4[K : \mathbb{Q}(\zeta)].$$

As $\gcd(4,5) = 1$, we have that 5 divides $[K : \mathbb{Q}(\zeta)]$. But α is a root of $x^5 - 2$ viewed as a polynomial in $\mathbb{Q}(\zeta)[x]$. So $[K : \mathbb{Q}(\zeta)] \leqslant 5$. We must have $[K : \mathbb{Q}(\zeta)] = 5$ and hence $[K : \mathbb{Q}] = 5 \times 4 = 20$.

Section C: Additional problems

—

Exercise 6.7

Show that if L/K is a Galois extension and $K \subseteq M \subseteq L$ is an intermediate field, then L/M is a Galois extension. [No work required, but take care to have addressed all parts of what it means to be Galois.]

For a finite field extension L/K, recall that the following are equivalent:

1) L is the splitting field of some separable polynomial $f \in K[x]$;
2) L/K is separable and normal;
3) $L^{\mathrm{Aut}_K L} = K$.

This modules takes (1) as the basic definition of a Galois extension and other equivalent forms as theorems. Using (1) in this question, we see that L is the splitting field of some separable $f \in K[x]$. That is, $L = K(\alpha_1, ..., \alpha_n)$ with $\alpha_1, ..., \alpha_n$ the roots of f. Since $K \subseteq M \subseteq L$, regarding f as a polynomial in $M[x]$, it is still separable and has the same roots: $L = M(\alpha_1, ..., \alpha_n)$. So L is also a splitting field of M, and hence L/M is a Galois extension.

Exercise 6.8

Compute the Galois group $\mathrm{Gal}(f)$ of $f = x^3 - 5 \in \mathbb{Q}[x]$.

Identify all subgroups of $\mathrm{Gal}(f)$ and draw the corresponding lattice of fixed fields. Identify all the normal field extensions of $\mathbb{Q}$ in the lattice of fixed fields, and confirm that they correspond to normal subgroups of $\mathrm{Gal}(f)$.

How do other normal field extensions in the lattice of fixed fields correspond to normal subgroups of certain other groups?

See Question 10 of Sheet 5.

Exercise 6.9

Let $f = x^4 - 2 \in \mathbb{Q}[x]$. Show that its splitting field $L \subseteq \mathbb{C}$ may be written $L = \mathbb{Q}(\alpha, i)$, with $\alpha = \sqrt[4]{2} \in \mathbb{R}$, and confirm $[L : \mathbb{Q}] = 8$.

Show that the following two maps

$$\sigma : \begin{cases} i \mapsto i \\ \alpha \mapsto i\alpha \end{cases} \quad \text{and} \quad \tau : \begin{cases} i \mapsto -i \\ \alpha \mapsto \alpha \end{cases}$$

are automorphisms, $\sigma, \tau \in \mathrm{Gal}(f) = \mathrm{Gal}(L/\mathbb{Q})$. [I find it useful to draw the field lattice of $L, \mathbb{Q}(\alpha), \mathbb{Q}(i), \mathbb{Q}$, and think about which extensions N/M are splitting fields for which irreducible polynomials. We have results that guarantee that certain permutations of roots of those polynomials are in $\mathrm{Aut}_M(N)$. Or one can check it by hand too, given that I've said what the answer is!]

Show they satisfy $\sigma^4 = \tau^2 = \mathrm{id}$ and $\tau\sigma = \sigma^3\tau$. Conclude that $\mathrm{Gal}(f) \cong D_8$, the dihedral group with 8 elements (a.k.a. the symmetry group of the square).

Calculate the subgroup lattice of D_8. [In terms of symmetries of the square, labelling the corners $1, 2, 3, 4$ cyclically and roots ordered $\alpha, i\alpha, -\alpha, -i\alpha$, we have $\sigma = (1234)$ and $\tau = (24)$.] [Hint2: five order 2 subgroups, three order 4.]

Compute the lattice of fixed subfields of L.

Over the splitting field L, f splits as

$$f(x) = x^4 - 2 = (x - \alpha)(x + \alpha)(x - \alpha \mathrm{i})(x + \alpha \mathrm{i}).$$

Hence $L = \mathbb{Q}(\alpha, -\alpha, \alpha\mathrm{i}, -\alpha\mathrm{i}) = \mathbb{Q}(\alpha, \alpha\mathrm{i}) = \mathbb{Q}(\alpha, \mathrm{i})$. By tower law,

$$[L : \mathbb{Q}] = [\mathbb{Q}(\alpha, \mathrm{i}) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

We have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = 4$ because f is irreducible over $\mathbb{Q}$ and hence is the minimal polynomial of α over $\mathbb{Q}$. Next, $[\mathbb{Q}(\alpha, \mathrm{i}) : \mathbb{Q}(\alpha)] = 2$ because $x^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}(\alpha)$. Therefore $[L : \mathbb{Q}] = 2 \times 4 = 8$.

To check that σ, τ are automorphisms of L, it suffices to check that they map roots of f to roots:

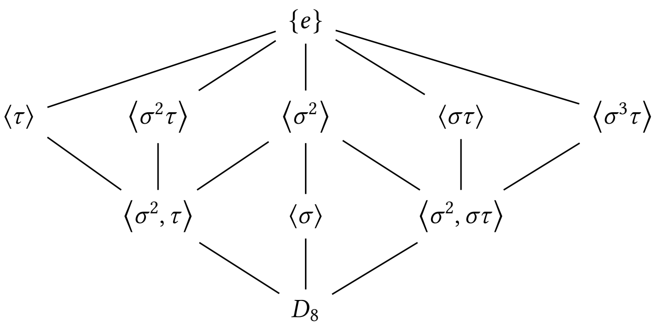
$$\sigma : \begin{cases} \alpha & \longmapsto \alpha\mathrm{i} \\ -\alpha & \longmapsto -\alpha\mathrm{i} \\ \alpha\mathrm{i} & \longmapsto -\alpha \\ -\alpha\mathrm{i} & \longmapsto \alpha \end{cases}, \qquad \tau : \begin{cases} \alpha & \longmapsto \alpha \\ -\alpha & \longmapsto -\alpha \\ \alpha\mathrm{i} & \longmapsto -\alpha\mathrm{i} \\ -\alpha\mathrm{i} & \longmapsto \alpha\mathrm{i} \end{cases}.$$

The automorphism τ is complex conjugation, so $\tau^2 = \mathrm{id}$; $\sigma : \alpha\mathrm{i}^n \mapsto \alpha\mathrm{i}^{n+1}$ permutes the four roots of f cyclically, thus $\sigma^4 = \mathrm{id}$. In fact on the square of the four roots $\alpha_n := \alpha\mathrm{i}^{n-1}$ on the complex plane, $\sigma = (1\ 2\ 3\ 4)$ is the rotation anti-clockwise by $\pi/2$ and $\tau = (2\ 4)$ is the reflection in the x-axis. It is clear that $\tau\sigma = \sigma^3\tau$ and $\langle\sigma, \tau\rangle \cong D_8 \leqslant \mathrm{Gal}(f)$. Note that $|D_8| = 8 = [L : \mathbb{Q}] = |\,\mathrm{Gal}(f)|$. Hence $\mathrm{Gal}(f) \cong D_8$.

Next we determine the subgroup lattice of D_8. The list of all element of D_8 is as follows:

- Order 1: e;
- Order 2: σ^2, τ, $\sigma\tau$, $\sigma^2\tau$, $\sigma^3\tau$;
- Order 4: σ, σ^3.

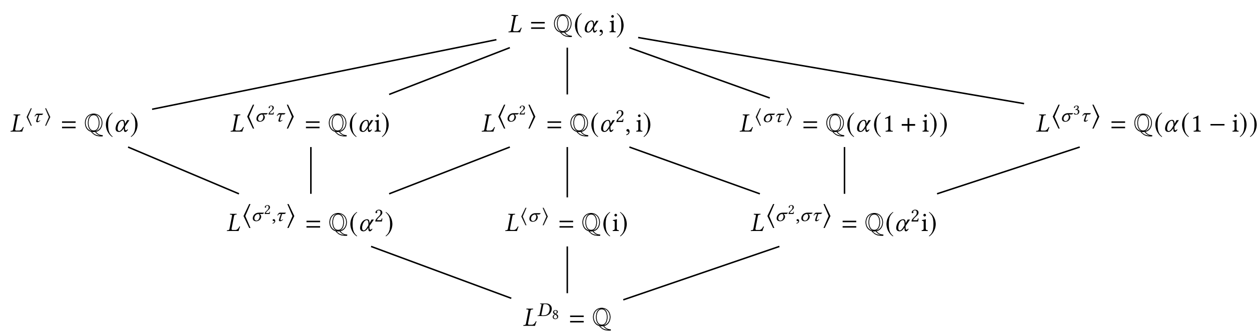
it is clear that each element of order 2 generates a distinct subgroup of D_8 of order 2, and this exhausts all the subgroups of order 2. For $H \leqslant D_8$ of order 4, if $H \cong C_4$ then $H = \langle\sigma\rangle = \langle\sigma^3\rangle$; if $H \cong C_2 \times C_2$, then $H = \langle\alpha, \beta\rangle$ for some elements α, β of order 2. Suppose that α, β are of the form $\sigma^i\tau$, $\sigma^j\tau$. Then $\sigma^{i-j} = \alpha\beta^{-1} \in H$. If $i - j$ is even, then $\sigma \in H$, which is impossible as H cannot have elements of order 4; if $i - j$ is odd, then $\sigma^2 \in H$. So in any case H is of the form $\langle\sigma^2, \sigma^i\tau\rangle$ for some i. We can check that $\langle\sigma^2, \tau\rangle = \langle\sigma^2, \sigma^2\tau\rangle \neq \langle\sigma^2, \sigma\tau\rangle = \langle\sigma^2, \sigma^3\tau\rangle$. In this way we have found all the non-trivial subgroups of D_8. They are organised in the following lattice:



To determine the fixed field of e.g. the subgroup $\langle\tau\rangle$, we write down a basis of L: $\{1, \alpha, \alpha^2, \alpha^3, \mathrm{i}, \alpha\mathrm{i}, \alpha^2\mathrm{i}, \alpha^3\mathrm{i}\}$. For $x = \sum_{j=0}^{3} c_j\alpha^j + \sum_{k=0}^{3} d_k\alpha^k\mathrm{i} \in L$,

$$x = \tau(x) \iff \sum_{j=0}^{3} c_j\alpha^j + \sum_{k=0}^{3} d_k\alpha^k\mathrm{i} = \sum_{j=0}^{3} c_j\alpha^j - \sum_{k=0}^{3} d_k\alpha^k\mathrm{i} \iff d_0 = d_1 = d_2 = d_3 = 0.$$

Hence $L^{\langle\tau\rangle} = \left\{\sum_{j=0}^{3} c_j\alpha^j \mid c_0, \ldots, c_3 \in \mathbb{Q}\right\} = \mathbb{Q}(\alpha)$. Other subfields of L can be computed in a similar way. The subfield lattice is shown below:



Each line in the diagram represents an extension of degree 2.

Exercise 6.10

Compute all the transitive subgroups of S_4. [Hint: there are five, up to conjugacy, of orders 4, 4, 8, 12, 24 respectively. "Up to conjugacy" means if you include $\langle(1234)\rangle$ you don't have to include $\langle(1324)\rangle$ and others achieved merely by relabelling the corners of the square.]

(You could also think about S_5. Again there are five, this time of orders 5, 10, 20, 60, 120. Good time to practice drawing pentagons and pentagrams.)

I will just do S_4. Let H be a transitive subgroup. By orbit–stabiliser theorem $4 \mid |H|$. From the subgroup lattice of S_4, we note that the subgroups of S_4 of order $4k$ are given up to conjugacy by:

$$\langle(1\ 2\ 3\ 4)\rangle \cong C_4; \quad \langle(1\ 2),\ (3\ 4)\rangle \cong V_4; \quad \langle(1\ 2)(3\ 4),\ (1\ 3)(2\ 4)\rangle \cong V_4; \quad \langle(1\ 2\ 3\ 4)(1\ 2)\rangle \cong D_8; \quad A_4; \quad S_4.$$

Since $\langle(1\ 2\ 3\ 4)\rangle \cong C_4$ acts on $\{1, 2, 3, 4\}$ by cyclic permutations, it is transitive. Therefore $\langle(1\ 2\ 3\ 4)(1\ 2)\rangle \cong D_8$, A_4 and S_4 are all transitive as they contain $\langle(1\ 2\ 3\ 4)\rangle$.

The subgroup $\langle(1\ 2),\ (3\ 4)\rangle$ is not transitive as $\{1, 2\}$ and $\{3, 4\}$ are two disjoint orbits under this action.

The subgroup $\langle(1\ 2)(3\ 4),\ (1\ 3)(2\ 4)\rangle = \{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$ is transitive. Checking is straightforward.

In summary, the transitive subgroups of S_4 are:

$$\langle(1\ 2\ 3\ 4)\rangle\,; \quad \langle(1\ 2)(3\ 4),\ (1\ 3)(2\ 4)\rangle\,; \quad \langle(1\ 2\ 3\ 4)(1\ 2)\rangle\,; \quad A_4; \quad S_4.$$