MA3D5 Galois Theory
Sheet 5 Solutions

Peize Liu

7 Nov 2024

Warn-up questions

Exercise 5.1. Definitions of the week.

Write, from memory, the definitions of irreducible polynomial, simple extension, degree of a field extension, splitting field and normal extension. Then check your notes to find the first mistake. Repeat until you have them correct 3 times in a row.

Exercise 5.2

Let $\varphi : L \longrightarrow L$ be an automorphism of a field L. Explain why the map φ^{-1} exists, and show that it is also an automorphism of L.

(E.g. to show $\varphi^{-1}(ab) = \varphi^{-1}(a)\varphi^{-1}(b)$ it may help to set $a = \varphi(x)$ and $b = \varphi(y)$ for some $x, y \in L$, which you can certainly do since φ is a bijection.)

See Question 3 of Sheet 4.

Exercise 5.3

Let $\varphi : L \longrightarrow L$ be a K-homomorphism of a finite extension L/K. Explain why the map φ is an automorphism of L - i.e. it is a bijection. [Hint: injective is easy since L is a field (6.1); surjective uses linear algebra, e.g. the rank-nullity theorem, once you observe that φ is also a K-linear map of K-vector spaces.]

A K-homomorphism is both a ring homomorphism and a K-linear map. Since φ is a ring homomorphism, its kernel $\ker \varphi$ is an ideal of L. Hence $\ker \varphi = \{0\}$ or L because L is a field. But $\varphi \neq 0$ as $\varphi|_K = \mathrm{id}$. Hence $\ker \varphi = \{0\}$. So φ is injective. On the other hand, φ is a linear transformation of the finite-dimensional K-vector space L. Since it is injective, it is also bijective, because $\operatorname{im} \varphi \cong L/\ker \varphi = L$ by the first isomorphism (i.e. rank–nullity theorem).

Exercise 5.4

Let $\sigma \in \mathrm{Aut}(L)$ be an automorphism of a field L. First write down the definition of the fixed field L^σ. Then show that $L^\sigma \subseteq L$ is a subfield of L. (i.e. check nonempty, closed under + and × and inverses.)

Show also that $L^H = L^\sigma$, where $H = \langle \sigma \rangle$ is the subgroup of Aut (L) generated by σ.

The first part is Question 7 of Sheet 4. For the second part, note that by definition

$$L^H = \bigcap_{\tau \in H} L^\tau \subseteq L^\sigma.$$

For the reverse inclusion, suppose that $x \in L^\sigma$. Then $\sigma(x) = x$. For any $\tau = \sigma^i \in H$, $\tau(x) = \sigma^i(x) = x$. Hence $x \in L^H$. This finishes the proof.

Exercise 5.5

If L/K has degree $[L : K]$ a prime, prove that L/K is a simple extension. [Hint: in fact, $L = K(\alpha)$ for any $\alpha \in L \setminus K$ follows very quickly from the Tower Law.]

See Question 10 of Sheet 4.

Problems for Week 6

Exercise 5.6

Let L/K be an extension and $K \subseteq M_i \subseteq L$ be two intermediate fields, with $i = 1, 2$.

(a) Show that $N = M_1 \cap M_2$ is also a field (obviously also $K \subseteq N \subseteq L$).

(b) Show that $M_1 \cup M_2$ is never a field unless $M_1 \subseteq M_2$ or $M_2 \subseteq M_1$.

These results should seem familiar to you in linear algebra.

(a) This is straightforward by checking the definition.

(b) Suppose that $M_1 \cup M_2$ is a field, $M_1 \not\subset M_2$ or $M_2 \not\subset M_1$. Then take $x \in M_1 \setminus M_2$ and $y \in M_2 \setminus M_1$. Then $x + y \notin M_1$ and $x + y \notin M_2$, because both M_1 and M_2 are fields. On the other hand, since $x, y \in M_1 \cup M_2$ and $M_1 \cup M_2$ is a field, we have $x + y \in M_1 \cup M_2$. This is a contradiction.

Exercise 5.7

Consider our basic example: $L = \mathbb{Q}(\alpha, \omega)$ with $\alpha = \sqrt[3]{2} \in \mathbb{R}$ and $\omega \in \mathbb{C}$ a primitive cube root of unity. Let $\sigma : L \longrightarrow L$ be complex conjugation, $\sigma(z) = \overline{z}$.

(a) Prove that σ is well defined; that is, $\sigma(\beta) \in L$ for all $\beta \in L$.

(b) Prove that σ is a homomorphism (of fields - i.e. it is a ring homomorphism). Note therefore that it is injective (prove this, if not obvious to you).

(c) Explain why $\sigma : L \longrightarrow L$ is both a $\mathbb{Q}$-homomorphism and a $\mathbb{Q}(\alpha)$-homomorphism.

(d) Prove that σ is surjective in two ways. [Hint. You could find two elements of L that map to α and ω respectively, and then use that σ is a K-homomorphism, or note that σ is an injective linear map of K-vector spaces $L \longrightarrow L$ (or of $K(\alpha)$ vector spaces, if you'd rather), and apply the rank-nullity formula.]

(a) (We assume (c) for this one.) Since σ is a $\mathbb{Q}$-homomorphism, it suffices to show that $\sigma(\alpha) \in L$ and $\sigma(\omega) \in L$. This is clear as

$$\sigma(\alpha) = \alpha; \qquad \sigma(\omega) = \overline{\omega} = \omega^2 \in L.$$

(b) This is straightforward by checking the definition. Also, $\overline{z} = 0$ if and only if $z = 0$ for all $z \in \mathbb{C}$. Hence σ is an injective ring homomorphism.

(c) $\sigma(z) = z$ for all $z \in \mathbb{R}$. Since $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{R}$, σ fixes all elements of $\mathbb{Q}$ and of $\mathbb{Q}(\alpha)$. This makes σ a $\mathbb{Q}$-(algebra)homomorphism and a $\mathbb{Q}(\alpha)$-(algebra)homomorphism.

(d) We have shown in Question 3 that any $\mathbb{Q}$-homomorphism of a finite extension $L/\mathbb{Q}$ is bijective.

Exercise 5.8

Let $G = S_3$, the group of permutations of $\{1, 2, 3\}$.

(a) Write out all elements of G.

(b) Check that $\sigma\tau\sigma^{-1} = (2, 3)$ where $\tau = (1, 2)$ and $\sigma = (1, 2, 3)$. More generally, recall that $\sigma\tau\sigma^{-1}$ is the same cycle type as τ, for any σ and τ, but with the entries replaced by their image under σ.

(c) Show that the pair $(1, 2)$ and $(1, 2, 3)$ generate G - that is, any element of G may be written as a combination of these (and their inverses, possibly with repeats).

(d) Find all the subgroups of G, and draw them in a subgroup lattice (as in Lecture 1), with inclusions down the page (so $\{\mathrm{id}\}$ will be at the top of your picture and G will be at the bottom).

This is purely group theory and these results are very standard. Let me omit this one.

Exercise 5.9

Let $L = \mathbb{Q}(\alpha, \omega)$ with $\alpha = \sqrt[3]{2} \in \mathbb{R}$ and $\omega \in \mathbb{C}$ a primitive cube root of unity. Show that $\mathbb{Q}(\alpha)$ is not the splitting field of any polynomial $g \in \mathbb{Q}[x]$. (Or equivalently, since $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a finite extension, that if is not a normal extension.)

Suppose that $\mathbb{Q}(\alpha)$ is the splitting field of $g \in \mathbb{Q}[x]$. Since α is a root of $x^3 - 2$, which is irreducible over $\mathbb{Q}$, by Theorem 9.9 in the notes, $x^3 - 2$ splits into linear factors over $\mathbb{Q}(\alpha)$. But this is impossible, as the two other roots $\alpha\omega, \alpha\omega^2$ are not real, and hence not in $\mathbb{Q}(\alpha)$.

Exercise 5.10

$L = \mathbb{Q}(\beta, \omega)$ with $\beta = \sqrt[3]{5} \in \mathbb{R}$ and $\omega \in \mathbb{C}$ a primitive cube root of unity.

(a) Show that L is the splitting field for $p = x^3 - 5 \in \mathbb{Q}[x]$.

(b) Compute the 3 roots of p in L, and call them $\beta_1, \beta_2, \beta_3$. Explain why any $\mathbb{Q}$-homomorphism of L must permute the β_i (either by proving this statement or by referring to relevant results from the lectures).

(c) Let $G = S_3$ act on L by permuting the 3 roots in the natural way (by permuting the indices of their names). You may assume that each such permutation extends to a $\mathbb{Q}$-automorphism of L (or you may prove that, either directly or by referring to results from the lectures). Find the fixed field L^H of each subgroup $H \subseteq G$.

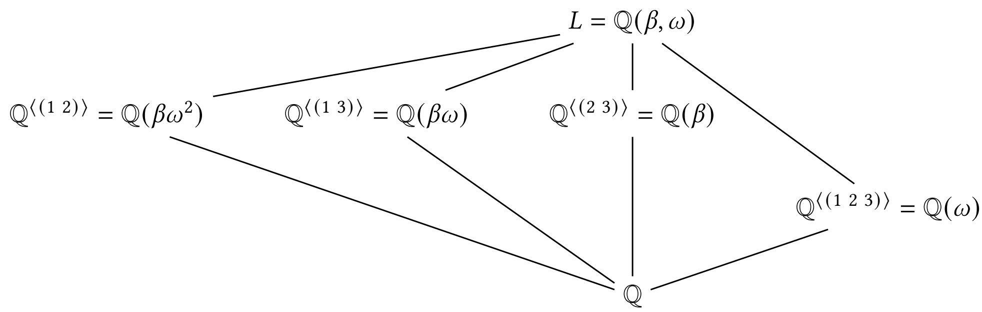
(d) Recall the definition of normal subgroup. Recall that if $H \subseteq S_n$ is a subgroup of a symmetric group S_n, then H is a normal subgroup if and only if H is a union of complete cycle types. (That is, for example, if H contains a 3-cycle (i, j, k) then it contains all 3-cycles; similarly for any other cycle type. This follows quickly from 8(b) above.)

(e) By inspecting each fixed field L^H, show that for this L and G, $H \subseteq G$ is a normal subgroup if and only if L^H is a normal extension of $\mathbb{Q}$.

(a) In the splitting field, $p(x) = x^3 - 5 = (x - \beta)(x - \beta\omega)(x - \beta\omega^2)$. Hence the splitting field of p is given by $\mathbb{Q}(\beta, \beta\omega, \beta\omega^2)$ as a subfield of $\mathbb{C}$. It is clear that $\mathbb{Q}(\beta, \beta\omega, \beta\omega^2) \subseteq L = \mathbb{Q}(\beta, \omega)$. For the reverse inclusion, just note that $\beta \in \mathbb{Q}(\beta, \beta\omega, \beta\omega^2)$ and also $\omega = \beta\omega/\beta \in \mathbb{Q}(\beta, \beta\omega, \beta\omega^2)$. Hence L is the splitting field of p.

(b) The three roots of p are $\beta_i = \beta\omega^{i-1}$ for $i = 1, 2, 3$. The fact that any $\mathbb{Q}$-homomorphism permutes the roots is **Fundamental Observation 6.35** in the notes.

(c) Any $\mathbb{Q}$-automorphism σ of $L = \mathbb{Q}(\beta_1, \beta_2, \beta_3)$ permutes the three roots. This gives a natural injection $\mathrm{Aut}(L) \hookrightarrow G = S_3$. We identify $\mathrm{Aut}(L)$ as a subgroup of G. To show that $\mathrm{Aut}(L) = G$, consider firstly the complex conjugation $\sigma_1 : z \longmapsto \bar{z}$. Under σ_1 we have $(\beta_1, \beta_2, \beta_3) \longmapsto (\beta_1, \beta_3, \beta_2)$. That is, $\sigma_1 = (2\,3) \in G$. Secondly, $\sigma_2\colon \begin{cases} \beta \mapsto \beta\omega \\ \omega \mapsto \omega \end{cases}$ induces a $\mathbb{Q}$-automorphism $\sigma_2\colon (\beta_1, \beta_2, \beta_3) \longmapsto (\beta_2, \beta_3, \beta_1)$. Hence $\sigma_2 = (1\,2\,3) \in G$. Since $(2\ 3)$ and $(1\ 2\ 3)$ generates G, we have $\mathrm{Aut}(L) = G$. In particular, every permutation of the roots $\{\beta_1, \beta_2, \beta_3\}$ extends to a $\mathbb{Q}$-automorphism. The subfield lattice of L is given by



(d) Note that any two different 2-cycles generate S_3. Hence the only non-trivial normal subgroup of S_3 is $\langle(1\ 2\ 3)\rangle$.

(e) The normal subgroups of G are $\{e\}$, $\langle(1\ 2\ 3)\rangle$, and G. The corresponding fixed fields $L^{\{e\}} = L$, $L^{\langle(1\ 2\ 3)\rangle} = \mathbb{Q}(\omega)$, and $L^G = \mathbb{Q}$ are normal; the non-normal subgroups of G are $\langle(1\ 2)\rangle$, $\langle(1\ 3)\rangle$, and $\langle(2\ 3)\rangle$. The corresponding fixed fields are not normal, which is clear from the lattice above.

Additional problems

Exercise 5.11

Factorise $x^7 - x \in K[x]$ into irreducible factors over each of the following fields:

(a) $K = \mathbb{Q}$

(b) $K = \mathbb{Q}(\omega)$

(c) $K = \mathbb{F}_2$

(d) $K = \mathbb{F}_7$

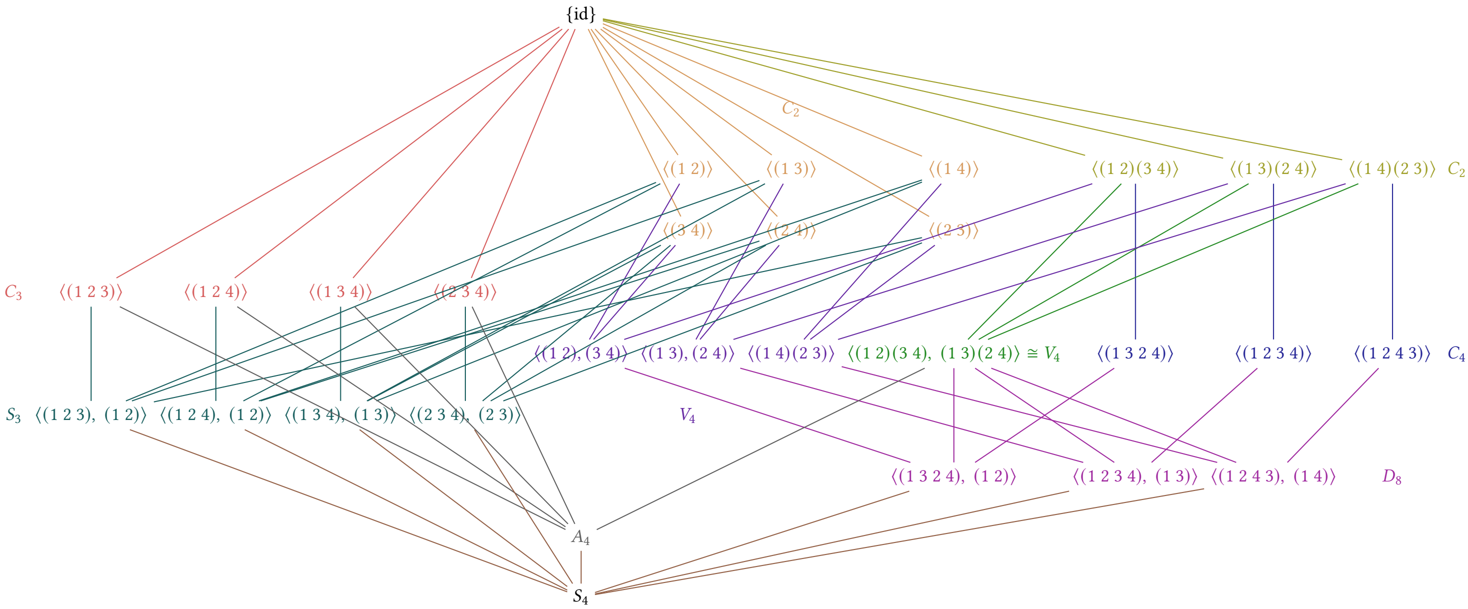
where $\omega \in \mathbb{C}$ is a primitive cube root of unity.

See Question 9 of Sheet 4.

Exercise 5.12

Repeat Q8 above with $G = S_4$. You can even do S_5 if you're brave.

There are 11 subgroups of S_4 up to conjugacy. The subgroup lattice of S_4 is given by



There are 19 subgroups of S_5 up to conjugacy. It would be impossible to draw the subgroup lattice of S_5 on the paper!