MA3D5 Galois Theory
Sheet 4 Solutions

Peize Liu

7 Nov 2024

Section A: Warn-up questions

Exercise 4.1

Show that $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$ for any θ. [E.g. use $\exp(3x) = \exp(x)^3$.]

Since $\exp(3\theta) = \exp(\theta)^3$, by Euler's formula we have

$$\begin{aligned}\cos(3\theta) + \mathrm{i}\sin(3\theta) &= (\cos\theta + \mathrm{i}\sin\theta)^3 \\ &= \cos^3\theta + 3\mathrm{i}\cos^2\theta\sin\theta - 3\cos\theta\sin^2\theta - \mathrm{i}\sin^3\theta.\end{aligned}$$

Taking the real parts of both sides:

$$\begin{aligned}\cos(3\theta) &= \cos^3\theta - 3\cos\theta\sin^2\theta \\ &= \cos^3\theta - 3\cos\theta(1-\cos^2\theta) \\ &= 4\cos^3\theta - 3\cos\theta.\end{aligned}$$

Exercise 4.2

Use the formula for the roots of a cubic to show that 4 is a root of $y^3 - 15y - 4$.

This is the standard cubic $y^3 + py + q$ with $p = -15$ and $q = -4$. The discriminant is given by

$$D = q^2 + \frac{4p^3}{27} = -484 = (22\mathrm{i})^2.$$

One of the root is therefore given by

$$\alpha = \sqrt[3]{\frac{-q+\sqrt{D}}{2}} + \sqrt[3]{\frac{-q-\sqrt{D}}{2}} = \sqrt[3]{2+11\mathrm{i}} + \sqrt[3]{2-11\mathrm{i}} = (2+\mathrm{i}) + (2-\mathrm{i}) = 4.$$

Exercise 4.3

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 is fine as φ is a bijection.)

In the notes a field automorphism φ is defined to be a bijection ring homomorphism between fields. Since φ is bijective, its inverse φ^{-1} exists as a map between the underlying sets. To check that it is also a ring homomorphism, pick $a, b \in L$. Set $a = \varphi(x)$ and $b = \varphi(y)$. Then $ab = \varphi(xy)$. Since φ is bijective,

$$\varphi^{-1}(ab) = xy = \varphi^{-1}(a) \cdot \varphi^{-1}(b).$$

In addition $\varphi^{-1}(1) = 1$ as $\varphi(1) = 1$. Hence φ^{-1} is a ring homomorphism.

Section B: Problems to hand in

Exercise 4.4

(a) Show that the polynomial $X^2 - 2$ is irreducible over $\mathbb{F}_3$.

(b) Let α be a root of $X^2 - 2$ in $\mathbb{F}_3[X]/(X^2 - 2)$. Show that the map $F : x \to x^3$ is an automorphism of $\mathbb{F}_3(\alpha)$ and determine $(\mathbb{F}_3(\alpha))^F$.

(c) Find the factorization of $X^{10} - 1$ in $\mathbb{Z}[X]$.

(a) If $x^2 - 2$ is reducible over $\mathbb{F}_3$, then $x^2 - 2 = (x - a)(x - b)$ for $a, b \in \mathbb{F}_3 = \{0, 1, 2\}$. But we can check that $x^2 - 2 \notin \{x^2, x(x-1), x(x-2), (x-1)^2, (x-1)(x-2), (x-2)^2\}$. Hence $x^2 - 2$ is irreducible.

(b) We have $\mathbb{F}_3[x]/\langle x^2 - 2 \rangle \cong \mathbb{F}_3(\alpha)$. In particular it is a field which is a finite extension of $\mathbb{F}_3$. To show that the Frobenius map $F : a \longmapsto a^3$ is an automorphism of $\mathbb{F}_3(\alpha)$, we need to check that it is a bijective ring homomorphism. Clearly $F(1) = 1$ and $F(ab) = a^3 b^3 = F(a)F(b)$. Since $\mathbb{F}_3(\alpha)$ has characteristic 3, we have

$$F(a + b) = (a + b)^3 = a^3 + 3a^2 b + 3ab^2 + b^3 = a^3 + b^3 = F(a) + F(b).$$

Hence it is a ring homomorphism. Since $\mathbb{F}_3(\alpha)$ is a field, $F(a) = a^3 = 0$ implies $a = 0$. Hence F is injective. Since $\mathbb{F}_3(\alpha)$ is a finite set, F is in fact bijective. This finishes the proof.

For $a \in (\mathbb{F}_3(\alpha))^F$, by definition we have $a^3 = a$. The solutions are exactly $\mathbb{F}_3 = \{0, 1, 2\}$. Hence $(\mathbb{F}_3(\alpha))^F = \mathbb{F}_3$.

(c) $(x^{10} - 1) = (x^5 - 1)(x^5 + 1) = (x - 1)(x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 - x^3 + x^2 - x + 1)$.

We claim that $f(x) = x^4 + x^3 + x^2 + x + 1$ and $g(x) = x^4 - x^3 + x^2 - x + 1$ are irreducible in $\mathbb{Z}[x]$. Note that $g(x) = f(-x)$, so it suffices to prove that f is irreducible. Note that f is the fifth cyclotomic polynomial and hence is irreducible by Example 5.8 in the notes. Explicitly, consider the polynomial $h(x) = f(x - 1)$. Since $f(x) = \dfrac{x^5 - 1}{x - 1}$, we have

$$h(x) = \frac{(x + 1)^5 - 1}{x} = x^4 + 5x^3 + 10x^2 + 10x + 5.$$

By Eisenstein's criterion with $p = 5$, h is irreducible in $\mathbb{Z}[x]$. Hence f is also irreducible. In conclusion, the factorisation of $x^{10} - 1$ we obtained is complete in $\mathbb{Z}[x]$.

Exercise 4.5

Let p be an odd prime and let $\omega \in \mathbb{C} \setminus \mathbb{R}$ be a root of $X^p - 1$.

(a) Show that $\mathrm{Aut}(\mathbb{Q}(\omega)) \neq \{\mathrm{id}\}$.

(b) Show that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ for all non-real roots α, β of $X^p - 1$.

(c) Bonus: (not graded) Show that $\mathrm{Aut}(\mathbb{Q}(\omega)) = (\mathbb{Z}/p\mathbb{Z})^*$.

(a) Recall that if $\varphi \in \mathrm{Aut}(K)$ and $\alpha \in K$, then α and $\varphi(\alpha)$ have the same minimal polynomial. In particular $\mathbb{Q}(\omega)$ permutes the roots of $x^p - 1$ which are included in $\mathbb{Q}(\omega)$. Clearly $\omega^2 \in \mathbb{Q}(\omega)$ is another root of $x^p - 1$ with $\omega \neq \omega^2$. Then $\varphi : \omega \longmapsto \omega^2$ induces an automorphism of $\mathbb{Q}(\omega)$ which is not the identity.

(b) This is similar to Question 5.(c) of Sheet 2. All the non-real roots of $x^p - 1$ are of the form $\zeta, \zeta^2, \ldots, \zeta^{p-1}$, where ζ is a primitve p-th root of unity. For any $i, j \in \{1, ..., p-1\}$, since $\gcd(j, p) = 1$, there exists $r \in \mathbb{Z}$ such that $\zeta^i = (\zeta^j)^r \in \mathbb{Q}(\zeta^j)$. It follows that $\mathbb{Q}(\zeta^i) = \mathbb{Q}(\zeta^j)$ for any i, j.

(c) We may take $\omega = \zeta$ to be one of the primitive roots, which generates all other roots. Consider the group homomorphism

$$\begin{aligned} (\mathbb{Z}/p\mathbb{Z})^\times &\longrightarrow \mathrm{Aut}(\mathbb{Q}(\omega)) \\ k &\longmapsto (\omega \longmapsto \omega^k) \end{aligned}$$

It is straightforward to check that this is bijective, as the image of ω completely determines an automorphism of $\mathbb{Q}(\omega)$.

Some cultural remarks. The same result generalises to any n, not just for odd prime p. Let ζ be a primitive n-th root of unity, where $n \geqslant 2$ is any integer. We claim that

$$\mathrm{Aut}(\mathbb{Q}(\zeta)) \cong (\mathbb{Z}/n\mathbb{Z})^\times \cong \mathbb{Z}/\phi(n)\mathbb{Z},$$

where $\phi(n)$ is the **Euler's totient function**, i.e. $\phi(n)$ is the size of the set $\{m \in \mathbb{Z}_{>0} \mid m < n,\ \gcd(n, m) = 1\}$.

The idea is to think of a field automorphism $\sigma \in \mathrm{Aut}(\mathbb{Q}(\zeta))$ as a permutation of the n-th roots of unity, and hence is a group automorphism of the cyclic group $\mu_n = \{\zeta^i \mid 0 \leqslant i \leqslant n-1\}$ of all n-th roots of unity. In particular we have an injection $\mathrm{Aut}(\mathbb{Q}(\zeta)) \hookrightarrow \mathrm{Aut}_{\mathsf{Grp}}(\mu_n)$. The latter satisfies

$$\mathrm{Aut}_{\mathsf{Grp}}(\mu_n) \cong \mathrm{Aut}_{\mathsf{Grp}}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times \cong \mathbb{Z}/\phi(n)\mathbb{Z},$$

which is a standard result in group theory. To show that $\mathrm{Aut}(\mathbb{Q}(\zeta)) \hookrightarrow \mathrm{Aut}_{\mathsf{Grp}}(\mu_n)$ is surjective, we may need a bit more Galois theory and some results about symmetric polynomials.

Note that $\mathbb{Q}(\zeta)$ contains all roots of $x^n - 1$, i.e. it is the splitting field of $x^n - 1$. Hence $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension, and hence $[\mathbb{Q}(\zeta) : \mathbb{Q}] = |\mathrm{Aut}(\mathbb{Q}(\zeta))| \leqslant |\mathrm{Aut}_{\mathsf{Grp}}(\mu_n)| = \phi(n)$. On the other hand, the n-th cyclotomic polynomial is given by

$$\Phi_n(x) := \prod_{\omega \text{ primitive } n\text{-th root}} (x - \omega).$$

It is a polynomial in $\mathbb{Q}(\zeta)[x]$ of degree $\phi(n)$, and its coefficients are symmetric polynomials in the primitve n-th roots of unity. Since any field automorphism $\sigma \in \mathrm{Aut}(\mathbb{Q}(\zeta))$ permutes the primitve n-th roots, the coefficients of Φ_n are fixed by σ. In particular, the coefficients

$$c_0, ..., c_n \in \mathbb{Q}^{\mathrm{Aut}(\mathbb{Q}(\zeta))} := \bigcap_{\sigma \in \mathrm{Aut}(\mathbb{Q}(\zeta))} \mathbb{Q}^\sigma = \mathbb{Q}.$$

Again we are using the fact that $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension. Hence $\Phi_n(x) \in \mathbb{Q}(x)$. It is clear that ζ is a root of $\Phi_n(x)$; on the other hand you can prove that $\Phi_n(x)$ is in fact irreducible over $\mathbb{Q}$ (the proof goes on for half more page but no need for more Galois theory). So $\Phi_n(x)$ is the minimal polynomial of ζ over $\mathbb{Q}$. It follows that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \Phi_n = \phi(n)$. We conclude that $|\mathrm{Aut}(\mathbb{Q}(\zeta))| = |\mathrm{Aut}_{\mathsf{Grp}}(\mu_n)|$ and the two groups are isomorphic.

Exercise 4.6

For an odd prime p, consider the polynomial $f = X^p - 2$. Let α be a root of f.

(a) Show that f is irreducible over $\mathbb{Q}$.

(b) Show that $\mathrm{Aut}(\mathbb{Q}(\alpha)) = \{\mathrm{id}\}$.

(a) Apply Eisenstein with the prime 2.

(b) Since an automorphism of $\mathbb{Q}(\alpha)$ permutes the roots of $x^p - 2$ that are included in $\mathbb{Q}(\alpha)$. To prove that $\mathrm{Aut}(\mathbb{Q}(\alpha)) = \{\mathrm{id}\}$, it suffices to show that $\mathbb{Q}(\alpha)$ does not contain other roots of $x^p - 2$. This is similar to Question 7.(c) of Sheet 2.

Suppose the contrary and let β be such a root. Then $(\beta/\alpha)^p = 1$ and $\beta/\alpha \neq 1$. We have $[\mathbb{Q}(\alpha) : \mathbb{Q}] =$

$p = [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha/\beta)][\mathbb{Q}(\alpha/\beta) : \mathbb{Q}]$ and thus $[\mathbb{Q}(\beta/\alpha) : \mathbb{Q}] = p$ or $[\mathbb{Q}(\beta/\alpha) : \mathbb{Q}] = 1$. In the first case we get a contradiction because $x^p - 1$ is reducible and so $[\mathbb{Q}(\alpha/\beta) : \mathbb{Q}] < p$. In the second case we get a contradiction because β/α is not real and is thus a root of $x^4+x^3+x^2+1$, which is an irreducible polynomial.

Exercise 4.7

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 $\times$ and inverses.)

As a subset, the fixed field is defined by

$$L^\sigma = \{x \in L \mid \sigma(x) = x\}.$$

It is non-empty because $0, 1 \in L^\sigma$. To check that it is a subfield, by the so-called 'subgroup test' it is enough to show that $a - b, ab^{-1} \in L^\sigma$ for $a, b \in L^\sigma$ ($b \neq 0$). This is clear, as σ is a ring homomorphism:

$$\sigma(a-b) = \sigma(a) - \sigma(b) = a - b; \qquad \sigma(ab^{-1}) = \sigma(a)\sigma(b)^{-1} = ab^{-1}.$$

Section C: Additional problems

Exercise 4.8

Write addition and multiplication tables (4×4 and 3×3 arrays, omitting 0 for multiplication) for the set $F = \{0, 1, a, b\}$ of four elements (where a and b are symbols), so that F is a field with those operations, with 0 and 1 behaving as the respective identities.

Do the same for the 4 elements of $G = \mathbb{F}_2[x]/\left(x^2 + x + 1\right)$.

Firstly, note that a finite field F contains $\mathbb{F}_p$ as a prime subfield for some $p = 2$, and hence $F \cong \mathbb{F}_p^n$ as an $\mathbb{F}_p$-vector space. Since $|F| = 4$, we have that $F \cong \mathbb{F}_2^2$ as a $\mathbb{F}_2$-vector space. In particular it has characteristic 2.

The elements of F are $0, 1, a, b$. Consider $c = a + 1 \in \{0, 1, a, b\}$. If $c = 0$, then $a = -1 = 1$; if $c = 1$, then $a = 0$; if $c = a$, then $0 = 1$. In all cases we obtain a contradiction. Hence $c = a + 1 = b$. This is enough to fix the addition table of F:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

For the multiplication, consider $d = a^2$. Since F is a field, if $d \neq 0$. If $d = 1$, then $a = 1$; if $d = a$, then $a(a - 1) = 0$ and hence $a = 0$ or $a = 1$. In both cases we have a contradiction. Hence $a^2 = b$. Similarly we have $b^2 = a$. Finally, $ab = a^2 + a = a + b = 1$. The multiplication is given by:

$\times$	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

For $G = \mathbb{F}_2[x]/\left\langle x^2 + x + 1\right\rangle$, we claim that this is a field. It suffices to show that $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$. It is clear, because the only linear polynomials of $\mathbb{F}_2[x]$ are x and $x + 1$, and it is straightforward to check that $x^2 + x + 1 \notin \{x^2, x(x + 1), (x + 1)^2\}$. Then G is a field with $[G : \mathbb{F}_2] = \deg(x^2 + x + 1) = 2$. So G is a field with 4 elements. We must have $G \cong F$ as the field structure on 4 elements is unique. The isomorphism is given by $\overline{x} \longmapsto a$ and $\overline{x+1} \longmapsto b$.

Exercise 4.9

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.

(a) $x^7 - x = x(x^6-1) = x(x^3-1)(x^3+1) = x(x-1)(x+1)(x^2+x+1)(x^2-x+1)$. We claim that x^2+x+1 and x^2-x+1 are irreducible over $\mathbb{Q}$. This can be checked either by showing that they have no rational roots or by modulo 2.

(b) Pick the primitive cube root of unity $\omega = \dfrac{-1+\sqrt{-3}}{2}$. So $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$. Then using the quadratic formula, we have

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

(c) Over $\mathbb{F}_2$ we have

$$x^7 - x = x(x-1)(x+1)(x^2+x+1)(x^2-x+1) = x(x+1)^2(x^2+x+1)^2.$$

We have shown that x^2+x+1 is irreducible over $\mathbb{F}_2$ in Q8.

(d) Note that $1 = -6$ in $\mathbb{F}_7$. Hence we have

$$\begin{aligned} x^7 - x &= x(x-1)(x+1)(x^2+x+1)(x^2-x+1) \\ &= x(x-1)(x+1)(x^2+x-6)(x^2-x-6) \\ &= x(x-1)(x+1)(x-2)(x+3)(x+2)(x-3) \\ &= x(x-1)(x-2)(x-3)(x-4)(x-5)(x-6). \end{aligned}$$

This is not a coincidence. In general, if K is field with $\operatorname{char} K = p$, then $\varphi : K \longrightarrow K$ given by $\alpha \longmapsto \alpha^p$ is a field automorphism, called the **Frobenius map**. Its restriction on the prime subfield $\mathbb{F}_p$ is the identity. That is, $\alpha^p = \alpha$ for all $\alpha \in \mathbb{F}_p$. Hence the polynomial $x^p - x$ splits into linear factors over $\mathbb{F}_p$ for any prime p, whose roots are exactly all the elements of $\mathbb{F}_p$.

Exercise 4.10

If L/K has degree $[L:K]$ a prime, prove that $L = K(\alpha)$ is a simple extension for any $\alpha \in L \setminus K$.

For any $\alpha \in L \setminus K$, we have $K \subsetneq K(\alpha) \subseteq L$. By tower law,

$$[L:K] = [L:K(\alpha)][K(\alpha):K] = p.$$

Since p is prime and $[K(\alpha):K] > 1$, then $[L:K(\alpha)] = 1$ and $[K(\alpha):K] = p$. Hence $L = K(\alpha)$ and $L \mid K$ is a simple extension.

Exercise 4.11

Go back to the polynomial $y^3 - 15y - 4$, which obviously has 4 as a root. Set $y = \lambda z$ and solve for λ to present the result as $z^3 - (3/4)z + c$. Check that $c \in [-1/4, 1/4]$, and use the trig formula to find the roots, rediscovering $y = 4$.

Consider the equation $y^3 - 15y - 4 = 0$. Substituting $y = \lambda z$, we have

$$z^3 - \frac{15}{\lambda^2}z - \frac{4}{\lambda^3} = 0.$$

Set $\frac{15}{\lambda^2} = \frac{3}{4}$, i.e. $\lambda = 2\sqrt{5}$. We obtain

$$z^3 - \frac{3}{4}z - \frac{1}{10\sqrt{5}} = 0.$$

Clearly $-\frac{1}{10\sqrt{5}} \in \left[-\frac{1}{4}, \frac{1}{4}\right]$. If we set $z = \cos\theta$, then by Q1 we have $z^3 - \frac{3}{4}z - \frac{1}{4}\cos(3\theta) = 0$. In particular we have $\cos(3\theta) = \frac{2}{5\sqrt{5}}$. Then all the real solutions is given by $y = \lambda\cos\left(\theta + \frac{2\pi}{3}k\right)$ for $k = 0, 1, 2$. To find $\cos\theta$ without solving the equation again, I have no choice but to seek help from plane geometry:

In the picture below, $\triangle OAB$ is a right triangle with $\cos\angle AOB = \frac{2}{5\sqrt{5}}$. Pick the point C on AB such that $AC = \frac{1}{11}AB$ and extend OC to the point E such that $OE = OB$. It is not difficult to see that $BC = BE$. As a result, $\angle AOC = \frac{1}{3}\angle AOB$. Hence $\cos\theta = \cos\angle AOC = \frac{OA}{OC} = \frac{2}{\sqrt{5}}$. It follows that $y = 2\sqrt{5} \cdot \frac{2}{\sqrt{5}} = 4$.