



## Solutions to Sample Test

November, 2025

1. (a) We have  $m(x) = x^2 - x + 1$ . The sixth roots of unity are roots of  $x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$ . Here
    - $x-1$  has as its root the primitive first root of unity, 1;
    - $x+1$  has as its root the primitive square root of unity,  $\zeta^3 = -1$ ;
    - $x^2+x+1$  has as its roots the primitive cube roots of unity,  $\zeta^2$  and  $\zeta^4$ ; and
    - $x^2-x+1$  has as its roots the primitive sixth roots of unity,  $\zeta$  and  $\zeta^5 = \zeta^{-1} = \bar{\zeta}$ .
 Of course the roots of  $m(x)$  are  $\frac{1 \pm \sqrt{-3}}{2}$  which are irrational, so  $m(x)$  is irreducible in  $\mathbb{Q}[x]$ .
  - (b) We have  $[E : \mathbb{Q}] = \deg m(x) = 2$ . One explicit choice of basis for  $E$  over  $\mathbb{Q}$  is  $\{1, \zeta\}$ ; another is  $\{1, \sqrt{-3}\}$ .
  - (c) From  $\zeta = e^{\pi i/3} = \frac{1}{2}(1 + \sqrt{-3})$  we get  $\sqrt{-3} = 2\zeta - 1 \in E$ .
  - (d) There are only two subfields of  $E$ , namely  $\mathbb{Q}$  and  $E$  itself. If  $F \subseteq E$  then  $F \supseteq \mathbb{Q}$  and  $2 = [E : \mathbb{Q}] = [E : F][F : \mathbb{Q}]$ . One of the latter two factors  $[E : F]$ ,  $[F : \mathbb{Q}]$  must be 1, and the other is 2. In one case,  $F = \mathbb{Q}$ ; in the other case,  $F = E$ .
2. If  $\pi^2$  is algebraic, then  $\pi$  is a root of a monic polynomial  $f(x) \in \mathbb{Q}[x]$ ; but then  $\pi$  is a root of the monic polynomial  $f(x^2) \in \mathbb{Q}[x]$ , a contradiction. So  $\pi^2$  is transcendental.
 

Now let  $\alpha = \sqrt{\pi}$  and suppose that  $\alpha$  is algebraic with minimal polynomial  $m(x) \in \mathbb{Q}[x]$  of degree  $n$ , say. That is,  $[\mathbb{Q}[\alpha] : \mathbb{Q}] = n$ . Since  $\pi = \alpha^2 \in \mathbb{Q}[\alpha]$ , the elements  $1, \pi, \pi^2, \dots, \pi^n \in \mathbb{Q}[\alpha]$  are linearly dependent over  $\mathbb{Q}$ . This gives a nonzero polynomial in  $\mathbb{Q}[x]$  having  $\pi$  as a root, a contradiction. So  $\alpha$  must be transcendental. (A much shorter argument uses the fact that the set of all algebraic numbers is a field  $\mathbb{A}$ , as indicated early in the semester. If  $\alpha \in \mathbb{A}$ , then  $\pi = \alpha^2 \in \mathbb{A}$ , a contradiction.)
  3. Since  $\alpha$  is a root of  $f(x)$ ,  $2\alpha+1$  is a root of  $f(\frac{x-1}{2}) = \frac{1}{8}m(x)$  where  $m(x) = x^3+3x^2-5x+9$ . So  $m(x)$  is the minimal polynomial of  $2\alpha+1$  over  $\mathbb{Q}$ .
 

The irreducibility of  $m(x)$  follows directly from the irreducibility of  $f(x)$ . (Because the change of variable  $x \mapsto \frac{x-1}{2}$  is invertible, factoring  $m(x)$  in  $\mathbb{Q}[x]$  would be equivalent to factoring  $f(x)$  in  $\mathbb{Q}[x]$ .) Alternatively, the irreducibility of  $m(x)$  in  $\mathbb{Q}[x]$  follows directly from the fact that  $m(\pm 1) \neq 0$ , so  $m(x)$  has no roots in  $\mathbb{Z}$ , so it has no roots in  $\mathbb{Q}$ .)
  4. The only two subfields of  $\mathbb{Q}[\alpha]$  are  $\mathbb{Q}$  and  $\mathbb{Q}[\alpha]$  itself. This is similar to #1(d): Every subfield  $F \subseteq \mathbb{Q}[\alpha]$  is an extension of  $\mathbb{Q}$ , so  $3 = [\mathbb{Q}[\alpha] : \mathbb{Q}] = [\mathbb{Q}[\alpha] : F][F : \mathbb{Q}]$ . Since 3 is prime, either  $[F : \mathbb{Q}] = 1$  or  $[\mathbb{Q}[\alpha] : F] = 1$ , which gives  $F = \mathbb{Q}$  or  $\mathbb{Q}[\alpha]$  respectively.

5. Dividing  $\alpha^3 + 3\alpha^2 + \alpha + 1 = 0$  by  $\alpha$  gives  $\alpha^2 + 3\alpha + 1 + \alpha^{-1}$ , so  $\alpha^{-1} = -1 - 3\alpha - \alpha^2$ .
6. (a) T (b) F (c) T (d) F (e) T (f) T (g) F (h) F (i) T (j) T

Some comments and explanations, provided for your benefit only (not required for answering #5):

- (a) Every subfield of  $\mathbb{R}$  contains  $\mathbb{Q}$ .
- (b) Consider the extension  $E \supset \mathbb{C}$  given by the field  $E = \mathbb{C}(x)$  of rational functions in an indeterminate  $x$ , with complex coefficients. Here  $[E : \mathbb{C}] = \infty$ .
- (c) This is easy to prove, directly from the axioms.
- (d) There is no subfield  $K \subset F$  of order 8, otherwise  $F$  is a vector space of dimension  $n = [F : K] \geq 1$  over  $K$ , and  $|F| = |K|^n$  gives  $16 = 8^n$ , which is impossible.
- (e) Let  $\{\alpha_1, \dots, \alpha_m\}$  be a basis for  $F$  over  $\mathbb{Q}$ , and let  $\{\beta_1, \dots, \beta_n\}$  be a basis for  $F'$  over  $\mathbb{Q}$ . Then the set of all products  $\alpha_i\beta_j$  spans an extension field  $E \supseteq \mathbb{Q}$  containing both  $F$  and  $F'$ . This is an exercise, and we note that  $[E : \mathbb{Q}] \leq mn$  so  $E$  is a finite extension of  $\mathbb{Q}$ . This looks very much like the proof of transitivity of degrees for field extensions; but we have only the inequality ' $\leq mn$ ' here since the products  $\alpha_i\beta_j$  are not necessarily linearly independent over  $\mathbb{Q}$  in this case. (For examples with inequality, consider for example the case when  $F' = F$  is a proper extension of  $\mathbb{Q}$ .)
- (f) Since  $\alpha = \frac{1 \pm \sqrt{13}}{2} \in \mathbb{Q}[\sqrt{13}]$ , we have  $\mathbb{Q}[\alpha] \subseteq \mathbb{Q}[\sqrt{13}]$ . The reverse inclusion follows just as easily since  $\sqrt{13} = \pm(-1 + 2\alpha) \in \mathbb{Q}[\alpha]$  implies  $\mathbb{Q}[\sqrt{13}] \subseteq \mathbb{Q}[\alpha]$ .
- (g) The degree  $[\mathbb{Q}[\zeta] : \mathbb{Q}] = \phi(n)$ , which is rather smaller than  $n$ . Here  $\phi$  is Euler's totient function. A simple example is  $n = 4$ , where  $\zeta = i$  generates an extension of degree 2.
- (h) It is easy to find elements of  $S$  that do not commute, e.g.  $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$  and  $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ .
- (i) Consider the extension  $E = \mathbb{Q}[2^{1/n}] \supseteq \mathbb{Q}$  of degree  $[E : \mathbb{Q}] = n$ , noting that the polynomial  $x^n - 2$  is irreducible in  $\mathbb{Q}[x]$ .
- (j) We have done similar examples to the in class. The minimal polynomial of  $\alpha$  over  $\mathbb{Q}$  is  $m(x) = x^4 - 10x^2 + 1$ .