Solutions to Practice Problems 1

October, 2024

1. $\alpha^3 = 2 + 3{\cdot}2^{4/3} + 3{\cdot}2^{5/3} + 4 = 6 + 6(2^{1/3} + 2^{2/3}) = 6 + 6\alpha$, so α is a root of $m(x) = x^3 - 6x - 6 \in \mathbb{Z}[x]$. This has no integer roots (any integer root would have to divide 6, but we easily check that $\pm1, \pm2, \pm3, \pm6$ are not roots of $m(x)$). So $m(x)$ is irreducible in $\mathbb{Z}[x]$, so it is irreducible in $\mathbb{Q}[x]$: it is the minimal polynomial of α over $\mathbb{Q}$.

2. Since $f(a) = a^4 + 1 > 0$ for all $a \in \mathbb{R}$, $f(x)$ has no real roots and certainly no rational roots. If it factors as a product of two quadratic factors in $\mathbb{Z}[x]$ then any such factorization must have the form $f(x) = (x^2 + ax + b)(x^2 - ax + b)$ where $a, b \in \mathbb{Z}$ (in order to avoid terms of degree 3). But then $b = \pm1$ and $2b - a^2 = 0$ so $a^2 = \pm2$ which has no integer solutions, a contradiction. We conclude that $f(x)$ is irreducible in $\mathbb{Z}[x]$ and also in $\mathbb{Q}[x]$.

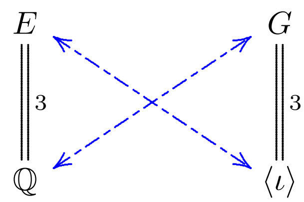
   Note that $\zeta^4 = -1$ so $\zeta^8 = 1$. We have $\mathbb{Q}[\zeta] \subseteq \mathbb{Q}[\zeta^3] \subseteq \mathbb{Q}[\zeta^9] = \mathbb{Q}[\zeta]$ so $E = \mathbb{Q}[\zeta] = \mathbb{Q}[\zeta^3]$. Similar arguments show $E = \mathbb{Q}[\zeta^5] = \mathbb{Q}[\zeta^7]$. In fact the roots of $f(x)$ are $\zeta, \zeta^3, \zeta^5, \zeta^7$ and so these four roots are conjugates. For $k \in \{1, 3, 5, 7\}$, denote by $\sigma_k : E \to E$ the automorphism which satisfies $\sigma_k(\zeta) = \zeta^k$. Such automorphisms exist since ζ^k $(k = 1, 3, 5, 7)$ are conjugates of ζ. These are all the automorphisms of E since any automorphism $\sigma \in \operatorname{Aut} E$ must map $\zeta \mapsto \zeta^k$ for some $k \in \{1, 3, 5, 7\}$, these being all the roots of $f(x)$; and since ζ generates the extension $E \supseteq \mathbb{Q}$, σ must coincide with σ_k. It is easy to see that $G = \operatorname{Aut} E = \{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}$ is a Klein four-group.

3. The similar example done in class, was the splitting field of $x^3 + x^2 - 2x - 1$, where the map $t \mapsto t^2 - 2$ was used to cycle the three roots. Other than the choice of polynomials, the details are the same and so I give a rather quick sketch of the proof; see the handout for further details. This example is useful for practicing the basic steps in studying Galois extensions.

   The polynomial $f(x) \in \mathbb{Q}[x]$ is irreducible in $\mathbb{Q}[x]$. (Otherwise it would have an integer root ±1, but $f(1) = -1$ and $f(-1) = 3$.) So we have a cubic extension $E = \mathbb{Q}[\alpha] \supset \mathbb{Q}$ where $\alpha \in \mathbb{C}$ is a root of $f(x) = x^3 - 3x + 1$. Then

$$\begin{aligned}
\alpha^3 &= 3\alpha - 1\\
\alpha^4 &= 3\alpha^2 - \alpha\\
\alpha^5 &= 3\alpha^3 - \alpha^2 \;=\; -\alpha^2 + 9\alpha - 3\\
\alpha^6 &= -\alpha^3 + 9\alpha^2 - 3\alpha \;=\; 9\alpha^2 - 6\alpha + 1.
\end{aligned}$$

Using these identities, it is easy to check that $f(2-\alpha-\alpha^2) = 0$, so the polynomial function $g(t) = 2-t-t^2$ permutes the three roots of $f(x)$. None of the roots can be fixed by g, otherwise that root would be a root of a quadratic polynomial $g(x)-x = 2-2x-x^2$, which is not divisible by $f(x)$. So g must permute the three roots $\alpha \mapsto \beta \mapsto \gamma \mapsto \beta$. Since $\beta = g(\alpha) \in \mathbb{Q}[\alpha]$, we have $\mathbb{Q}[\beta] \subseteq \mathbb{Q}[\alpha]$. The same argument shows that $\mathbb{Q}[\beta] \subseteq \mathbb{Q}[\alpha] \subseteq \mathbb{Q}[\gamma] \subseteq \mathbb{Q}[\beta]$, so in fact $\mathbb{Q}[\alpha] = \mathbb{Q}[\beta] = \mathbb{Q}[\gamma] = E$. So the map $\sigma : E \to E$ defined by $\sigma(a+b\alpha+c\alpha^2) = a+b\beta+c\beta^2$ (for all $a, b, c \in \mathbb{Q}$) is an automorphism of E. (*Warning*: Although σ permutes the three roots in the same way that g does, $\sigma(t) \neq g(t)$ for other elements $t \in E$. The map $E \to E$, $t \mapsto g(t)$ is not even one-to-one, e.g. $g(-2) = g(1) = 0$. Of course, $\sigma(-2) = -2$ and $\sigma(1) = 1$.) The group $G = \operatorname{Aut} E = \langle\sigma\rangle = \{\iota, \sigma, \sigma^2\}$ is cyclic of order 3 and so we call $E \supset \mathbb{Q}$ a cyclic cubic extension.



4. Let $E \supset \mathbb{Q}$ be a quadratic extension, with basis $\{1, \alpha\}$. Since $\alpha^2 \in E$, we have $\alpha^2 = k + \ell\alpha$ for some $k, \ell \in \mathbb{Q}$. After multiplying by the least common multiple of the denominators, we find that α is a root of $ax^2 + bx + c$ for some $a, b, c \in \mathbb{Z}$; so $\alpha = \frac{1}{2a}(-b\pm\sqrt{d})$ where $d = b^2-4ac \in \mathbb{Z}$. Clearly $E = \mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{d}\,]$. If $d \not\equiv 0 \mod 4$, we are done. Otherwise $d = 4^k m$ for some $k \geqslant 1$ and $m \not\equiv 0 \mod 4$. In this case, $E = \mathbb{Q}[\sqrt{d}\,] = \mathbb{Q}[2^k\sqrt{m}\,] = \mathbb{Q}[\sqrt{m}\,]$ and once again, we are done.

5. This example is attributed to Daniel Shanks, who was the first person to compute the first 100,000 decimal places of π. I have no idea how he found the remarkable identity in (b).

   (a) We have
$$\begin{aligned}
\alpha - \sqrt{5} &= \sqrt{22 + 2\sqrt{5}} \\
\alpha^2 - 2\alpha\sqrt{5} + 5 &= 22 + 2\sqrt{5} \\
\alpha^2 - 17 &= 2(\alpha + 1)\sqrt{5} \\
(\alpha^2 - 17)^2 &= 20(\alpha + 1)^2 \\
\alpha^4 - 34\alpha^2 + 289 &= 20\alpha^2 + 40\alpha + 20 \\
\alpha^4 - 54\alpha^2 - 40\alpha + 269 &= 0,
\end{aligned}$$
   so α is a root of $m(x) = x^4 - 54x^2 - 40x + 269 \in \mathbb{Q}[x]$. You can use the usual procedure to show that $m(x)$ is irreducible in $\mathbb{Q}[x]$; but let me show you a trick that simplifies the arithmetic. The substitution $y = 4x + 3$, i.e. $x = \frac{y-3}{4}$, allows us to rewrite $m(x) = 256f(y)$ where $f(y) = y^4 + 3y^3 - 4y - 1$. Now $m(x)$ is irreducible in $\mathbb{Q}[x]$ iff $f(y)$ is irreducible in $\mathbb{Q}[y]$. (Any nontrivial factorization $m(x) = m_1(x)m_2(x)$ in $\mathbb{Q}[x]$ gives a nontrivial factorization $f(y) = f_1(y)f_2(y)$ in

$\mathbb{Q}[y]$, and conversely.) It suffices to show that $f(y)$ has no nontrivial factorization in $\mathbb{Z}[y]$. First, $f(y)$ has no linear factors in $\mathbb{Z}[y]$, otherwise it would have a root in $\mathbb{Z}$ dividing 1; but both $f(1) = -1$ and $f(-1) = 1$ are nonzero, so this cannot happen. If $f(y)$ factors into quadratic factors in $\mathbb{Z}[y]$, then

$$f(y) = y^4 + 3y^2 - 4y - 1 = (y^2 + ay - 1)(y^2 + by + 1)$$

for some $a, b \in \mathbb{Z}$. From the coefficients of y^3 and y, we get $a + b = 3$ and $a-b = -4$. Adding these equations gives $2a = -1$, which is not possible for $a \in \mathbb{Z}$. This contradiction proves that $f(y) \in \mathbb{Q}[y]$ and so $m(x) \in \mathbb{Q}[x]$ is irreducible. So $m(x)$ is the minimal polynomial of α over $\mathbb{Q}$.

(b) I will denote the given expression by $\theta = \sqrt{u} + \sqrt{v + 2\sqrt{w}}$ where

$$u = 11 + 2\sqrt{29}, \qquad v = 16 - 2\sqrt{29}, \qquad w = 55 - 10\sqrt{29}.$$

The fact that $u, v, w \in \mathbb{Q}[\sqrt{29}]$ will be helpful in these calculations. In particular, note that $uw = 25$. My strategy is to show that θ has the same minimal polynomial over $\mathbb{Q}$ as α. Using calculus, we see that $m(x)$ has four real roots, one on each of the intervals $[-7, -6]$, $[-3, -2]$, $[1, 2]$, $[7, 8]$. Numerical estimates show that $\alpha, \theta \in [7, 8]$, so they are both equal to the largest root of $m(x)$. This gives $\alpha = \theta$. Now

$$\begin{aligned}
\theta - \sqrt{u} &= \sqrt{v + 2\sqrt{w}} \\
\theta^2 - 2\theta\sqrt{u} + u &= v + 2\sqrt{w} \\
\theta^2 + u - v &= 2\theta\sqrt{u} + 2\sqrt{w} \\
(\theta^2 + u-v)^2 &= (2\theta\sqrt{u} + 2\sqrt{w})^2 \\
\theta^4 + 2(u-v)\theta^2 + (u-v)^2 &= 4u\theta^2 + 8\theta\sqrt{uw} + 4w \\
\theta^4 + 2(u-v)\theta^2 + (u-v)^2 &= 4u\theta^2 + 40\theta + 4w \\
\theta^4 + [2(u-v)-4u]\theta^2 - 40\theta + [(u-v)^2-4w] &= 0 \\
\theta^4 - 54\theta^2 - 40\theta + 269 &= 0.
\end{aligned}$$

Here we have carefully calculated the coefficients using arithmetic in $\mathbb{Q}[\sqrt{29}]$; and it follows that $\theta = \alpha$ as explained above.

6. From $m(x) = x^3 - 7x^2 + 5x - 3 = (x - \alpha)(x - \beta)(x - \gamma)$ we obtain

$$\alpha + \beta + \gamma = 7, \qquad \alpha\beta + \alpha\gamma + \beta\gamma = 5, \qquad \alpha\beta\gamma = -3.$$

This answers (a) and (b). As for (c), we have

$$\alpha^2 + \beta^2 = \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \alpha\gamma + \beta\gamma) = 7^2 - 2 \cdot 5 = 39.$$

The fact that all these values are rational follows from the fact that each of the expressions is fixed by the Galois group of the polynomial (since permuting α, β, γ does not change them). The fact that they are all integers follows from knowing a little more algebra beyond what we are covering in our course: Not only are α, β, γ

algebraic numbers (i.e. roots of nonzero polynomials with integer coefficients), they are in fact *algebraic integers* (i.e. roots of *monic* polynomials with integer coefficients).

7. This exercise uses the isomorphism $E = \mathbb{Q}[\alpha]$ to a subring of the 3×3 rational matrices, where α is a root of $m(x) = x^3+x^2-2x-1$. As studied in class, $m(x)$ has three roots α, β, γ which are permuted cyclically by $t \mapsto t^2 - 2$. From
$$x^3 + x^2 - 2x - 1 = (x-\alpha)(x-\beta)(x-\gamma)$$
we obtain
$$\alpha+\beta+\gamma = -1, \qquad \alpha\beta+\alpha\gamma+\beta\gamma = -2, \qquad \alpha\beta\gamma = 1.$$
The isomorphism from E to a subring of $\mathbb{Q}^{3\times3}$ maps α, β, γ to a triple of matrices A, B, C satisfying exactly the same relations. You can find one of the three matrices using a companion matrix for $m(x)$, as I have explained earlier;then generate the other two using the cyclic action of $t \mapsto t^2 - 2$ on the roots. One possible solution is
$$A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 1 & -1 \end{bmatrix}, \qquad B = \begin{bmatrix} -2 & 1 & -1 \\ 0 & 0 & -1 \\ 1 & -1 & 1 \end{bmatrix}, \qquad C = \begin{bmatrix} 1 & -1 & 0 \\ -1 & -1 & -1 \\ -1 & 0 & -1 \end{bmatrix}.$$

8. (a) $i^i = (e^{(2n+\frac{1}{2})\pi i})^i = e^{-(2n+\frac{1}{2})\pi}$ for $n \in \mathbb{Z}$. Interestingly, all possible values of i^i are real.

   (b) The values $\alpha = \sqrt{2}^{\sqrt{2}}$ and $\beta = \sqrt{2}$ are irrational. (By the Gelfond-Schneider Theorem, α is in fact transcendental.) Also $\alpha^\beta = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$ is rational.

9. First observe that $\alpha = \pi^2-1$ is transcendental. This is because any polynomial in α (with rational coefficients) is a polynomial in π (with rational coefficients). Even more bluntly, if a nonzero polynomial $g(x) \in \mathbb{Q}[x]$ of degree $n \geqslant 1$ satisfies $g(\alpha) = 0$, then $f(\pi) = 0$ where $f(x) = g(x^2-1)$. And $\deg f(x) = 2n \geqslant 2$, so this is also a nonzero polynomial. This is a contradiction.

   Next, suppose $\sqrt{\alpha}$ is algebraic; and let $h(x) \in \mathbb{Q}[x]$ be a nonzero polynomial having $h(\sqrt{\alpha}) = 0$. The polynomial $f(x) = h(x)h(-x)$ is also nonzero (its degree is twice the degree of $h(x)$) and $f(x)$ is an even polynomial (i.e. $f(-x) = f(x)$). This means that every term appearing in $f(x)$ has even degree, i.e. $f(x) = p(x^2)$ for some nonzero polynomial $p(y) \in \mathbb{Q}[y]$. And $p(\alpha) = f(\sqrt{\alpha}) = h(\sqrt{\alpha})h(-\sqrt{\alpha}) = 0$, a contradiction. So $\sqrt{\alpha} = \sqrt{\pi^2-1}$ is also transcendental.

   We don't actually have to be this clever. There are much easier ways to answer the question, after we cover some more basic results. An extension $E \supseteq F$ is *algebraic* if every $\alpha \in E$ is algebraic over F (i.e. there exists a nonzero $f(x) \in F[x]$ such that $f(\alpha) = 0$). Every finite extension is algebraic. And given a tower of extensions $E \supseteq K \supseteq F$, the extension $E \supseteq F$ is algebraic iff both of the extensions $E \supseteq K$ and

$K \supseteq F$ are algebraic. And given an element α in some extension of F, the element α is algebraic over F iff the extension $F(\alpha) \supseteq F$ is algebraic. These facts are ... well, not too hard to prove. Now consider $\beta = \sqrt{\pi^2-1} = \sqrt{\alpha}$ where $\alpha = \pi^2-1$. Then $\beta \in K(\beta) \supseteq K \supseteq \mathbb{Q}$ and $\pi \in K(\pi) \supseteq K \supseteq \mathbb{Q}$ where $K = \mathbb{Q}(\alpha)$. The extension $K(\pi) \supseteq \mathbb{Q}$ cannot be algebraic since it contains a transcendental element π. But $K(\pi) \supseteq K$ is algebraic since π is a root of $x^2 - \alpha \in K[x]$. So the extension $K \supseteq \mathbb{Q}$ cannot be algebraic. In particular, the extension $K(\pi) = \mathbb{Q}(\pi) \supseteq \mathbb{Q}$ cannot be algebraic.

10. Numerical evaluation of the sequence of approximations $\sqrt{2}$, $\sqrt{2}^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{2}^{\sqrt{2}}}$, ... leads us to conjecture that the limit is 2. The decimal approximations also lead us to believe that the sequence is increasing, which suggests the following plan of attack.

    Define $f(x) = 2^{x/2} = \sqrt{2}^{\,x}$. Whenever $0 < x < 2$, we have $0 < x < f(x) < 2$. (Use $f(x) = 2^{x/2} < 2^1 = 2$. Also by the first derivative test, the function $g(x) = \frac{\ln x}{x}$ is increasing on the interval $(0, e]$, so $\frac{\ln x}{x} < \frac{\ln 2}{2}$ and $x = e^{\ln x} < e^{(x \ln 2)/2} = f(x)$.) Our sequence of approximations is $f(1), f(f(1)), f(f(f(1))), \ldots$ which is an increasing sequence of real numbers less than 2. So it converges to a real number $\alpha \leqslant 2$. This number satisfies $\alpha = f(\alpha)$, so $\ln \alpha = \ln f(\alpha) = \frac{\alpha \ln 2}{2}$, i.e. $g(\alpha) = g(2)$. Again using the fact that $g(x)$ is increasing on the interval $(0, e]$, this forces $\alpha = 2$. Of course this value is rational.

11. The required value α satisfies $\alpha = \sqrt{5+\sqrt{5-\alpha}}$, so $\alpha^2 = 5+\sqrt{5-\alpha}$, $\alpha^2-5 = \sqrt{5-\alpha}$ and $\alpha^4-10\alpha^2+25 = 5-\alpha$. So α is a root of

$$x^4 - 10x^2 + x + 20 = (x^2 + x - 5)(x^2 - x - 4).$$

    Thus $\alpha \in \left\{\frac{1}{2}\left(-1\pm\sqrt{21}\right), \frac{1}{2}\left(1\pm\sqrt{17}\right)\right\}$. However, it is evident from the original expression for α that we must have $\alpha > \sqrt{5}$. Only one of the four roots satisfies this requirement, giving $\alpha = \frac{1}{2}\left(1+\sqrt{17}\right)$. This value is algebraic of degree two (a quadratic irrational) with minimal polynomial $x^2 - x - 4$ over $\mathbb{Q}$.

    Remarks. This identity for α is unexpected, much as Shanks' identity in #5(b) is unexpected. An important point here is that after finding a monic polynomial in $\mathbb{Z}[x]$ having α as a root, we would usually expect this to be the minimal polynomial. This example reminds us, however, not to jump too quickly to this conclusion.

12. This example relates to straightedge-and-compass constructions, which we will discuss in class. We have a tower of extension fields

$$E_n \supseteq E_{n-1} \supseteq \cdots \supseteq E_2 \supseteq E_1 \supseteq E_0 = \mathbb{Q}$$

    where $E_i = E_{i-1}[a_i\sqrt{b_i}]$ for $i = 1, 2, \ldots, n$. Since $a_i\sqrt{b_i}$ is a root of the quadratic polynomial $x^2 - a_i^2 b_i \in E_{i-1}[x]$, we have $[E_i : E_{i-1}] \leqslant 2$. By transitivity of degrees of extensions, $[E_n : \mathbb{Q}] = 2^k$ for some $k \in \{0, 1, 2, \ldots, n\}$. Now consider the element $\beta \in E_n$ defined by $\beta = \sum_{i=1}^{n} a_i\sqrt{b_i}$. Since $E_n \supseteq \mathbb{Q}[\beta] \supseteq \mathbb{Q}$, $[\mathbb{Q}[\beta] : \mathbb{Q}]$ must divide $[E_n : \mathbb{Q}] = 2^k$. However, $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$, so $\beta \neq \alpha$.