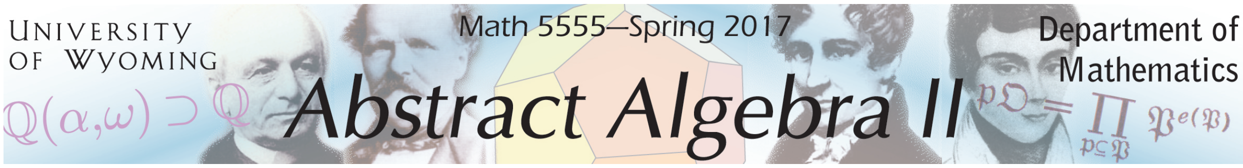


Solutions to HW1

1. Every element $u = a + b\varepsilon \in R$ with $a \neq 0$ is a unit since it has inverse $u^{-1} = \frac{a-b\varepsilon}{a^2}$. No proper ideal contains a unit; if an ideal J contains a unit u then $R = R1 = Ruu^{-1} \subseteq Ju^{-1} \subseteq J$ forcing $J = R$. Thus every proper ideal satisfies $J \subseteq (\varepsilon)$ where $(\varepsilon) = R\varepsilon = \{b\varepsilon : b \in F\}$. However, $(\varepsilon) \subset R$ is an ideal since it is a principal ideal. In order for the ideal J to be maximal, it must satisfy $J = (\varepsilon)$.

2. Let $f(X) \in F[X]$ be a polynomial of degree 2. Without loss of generality, $f(X)$ is monic; otherwise divide $f(X)$ by its leading coefficient without changing the principal ideal $(f(X)) \subset F[X]$. Now $f(X)$ has 0, 1 or 2 distinct roots in F. Denote the quotient ring $R = F[X]/(f(X))$.

   If $f(X)$ has no roots in F, then it is irreducible in $F[X]$ so the ideal $(f(X)) \subset F[X]$ is maximal. This means that the quotient ring R is a field. Denoting $\alpha = X + (f(X)) \in R$, every element of R is uniquely expressible as $a + b\alpha$ for some $a, b \in F$. (Simply take an arbitrary coset $g(X) + (f(X)) \in R$ and represent it by the remainder of $g(X)$ found after dividing by $f(X)$. This remainder $a + bX$ is unique.) Thus $[R : F] = 2$ and so conclusion (ii) holds.

   If $f(X)$ has one double root in F then $f(X) = (X - r)^2$ for some $r \in F$. Without loss of generality $r = 0$. (The map $F[X] \to F[X + r]$, $g(X) \mapsto g(X + r)$ is a ring isomorphism mapping the ideal $((X - r)^2)$ to the ideal (X^2).) In this case $R = F[X]/(X^2)$. Denote $\varepsilon = X + (X^2) \in R$. Every coset $g(X) + (X^2) \in R$ is uniquely expressible as $a + b\varepsilon$ where $a, b \in F$. (Again, find the remainder $a + bX$ of $g(X)$ after dividing by X^2 to obtain the unique representative.) Now R is a two-dimensional vector space over F with basis $\{1, \varepsilon\}$ satisfying $\varepsilon^2 = 0$. This gives case (iii).

   Finally, suppose $f(X)$ has two distinct roots in F, so $f(X) = (X - r_1)(X - r_2)$ for distinct roots $r_i \in F$. Consider the ideals $J_1 = (X - r_i) \subset F[X]$, $i = 1, 2$. Observe that $J_1 J_2 = J_1 \cap J_2 = (f(X)) \subset F[X]$. It is easy to see that

   $$(*) \qquad F[X]/(f(X)) \;=\; F[X]/(J_1 \cap J_2) = \big(F[X]/J_1\big) \oplus \big(F[X]/J_2\big).$$

   Indeed, the map $\phi : F[X] \mapsto \big(F[X]/J_1\big) \oplus \big(F[X]/J_2\big)$ defined by $g(X) \mapsto (g(X) + J_1, g(X) + J_2)$ is a ring homomorphism since each of the maps $F[X] \to F[X]/J_i$ is a ring homomorphism. Since the kernel of ϕ is $J_1 J_2 = J_1 \cap J_2$, the first isomorphism theorem gives (*). Now use the fact that $F[X]/J_i \cong F$ (each $X - r_i$ is irreducible of degree 1) to obtain case (i).

3. (a) In this case $f(x) = (x+\alpha+\beta)(x-\alpha-\beta)(x+\alpha-\beta)(x-\alpha+\beta)$ where $\alpha = i\sqrt{2}$ and $\beta = i\sqrt{5}$. The splitting field of $f(x)$ over $\mathbb{Q}$ is

$$E = \mathbb{Q}(\pm\alpha \pm \beta) = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, \sqrt{10})$$

since $\alpha\beta = -\sqrt{10}$. The extension $K = \mathbb{Q}(\sqrt{10}) \supseteq \mathbb{Q}$ has degreee 2 since 10 is not a perfect square in $\mathbb{Q}$; and $E = K(\alpha) \supseteq K$ has degree 2 ($[E:K] \leqslant 2$ since α is a root of $t^2+2 \in K[t]$; but $[E:K] > 1$ since $K \subset \mathbb{R}$ whereas $\alpha \in E$ is not real). This shows that $[E:\mathbb{Q}] = 4$. Since E is the splitting field of $f(t) \in \mathbb{Q}[t]$, $E \supset \mathbb{Q}$ is Galois and hence $|G| = [E:\mathbb{Q}] = 4$. Since every automorphism of E maps $\alpha \mapsto \pm\alpha$ and $\beta \mapsto \pm\beta$, the only possibility is $G = \{\iota, \sigma, \tau, \sigma\tau\}$, a Klein 4-group satisfying $\sigma(\alpha) = -\alpha$, $\sigma(\beta) = \beta$, $\tau(\alpha) = \alpha$, $\tau(\beta) = -\beta$.

(b) By Eisenstein's Criterion (for the prime 2), $f(x)$ is irreducible over $\mathbb{Q}$. Note that $f(x) = (x+\alpha)(x-\alpha)(x+\beta)(x-\beta)$ where $\alpha = \sqrt{2-\sqrt{2}}$ and $\beta = \sqrt{2+\sqrt{2}}$; so $f(x)$ is the minimal polynomial over $\mathbb{Q}$ for each of its four roots. Since $\beta = \alpha(3-\alpha^2)$, we have $E = \mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha)$. Since E is the splitting field of $f(x)$ over $\mathbb{Q}$, the extension $E \supset \mathbb{Q}$ is Galois of degree 4. Every $g \in G$ maps α to one of the four roots of $f(x)$ and the choice of $g(\alpha) \in \{\pm\alpha, \pm\beta\}$ uniquely determines g since α generates the extension $E \supset \mathbb{Q}$. Denote by $\sigma \in G$ the unique automorphism mapping $\alpha \mapsto \beta$; then

$$\sigma^2(\alpha) = \sigma(\beta) = \sigma\big(\alpha(3-\alpha^2)\big) = \beta(3-\beta^2) = -\alpha;$$
$$\sigma^3(\alpha) = \sigma(-\alpha) = -\beta$$

so $G = \langle\sigma\rangle = \{\iota, \sigma, \sigma^2, \sigma^3\}$ is cyclic of order 4 where the generator σ cyclically permutes the roots of $f(x)$ as

$$\alpha \mapsto \beta \mapsto -\alpha \mapsto -\beta \mapsto \alpha.$$

4. Suppose $\alpha \in \mathbb{Q}_p$ satisfies $\alpha^2+\alpha+1 = 0$. If $c = \|\alpha\|_p > 1$ then

$$c^2 = \|\alpha^2\|_p = \|-\alpha-1\|_p = \max\{c, 1\},$$

which is impossible; so we must have $\|\alpha\|_p \leqslant 1$, i.e. $\alpha \in \mathbb{Z}_p$. Now reducing the equation $\alpha^2+\alpha+1 = 0$ mod p or mod p^2, gives zeroes of X^2+X+1 in $\mathbb{Z}_p/pZ_p \cong \mathbb{Z}/p\mathbb{Z}$ and in $\mathbb{Z}_p/p^2Z_p \cong \mathbb{Z}/p^2\mathbb{Z}$. But we quickly check that X^2+X+1 has no zeroes in $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$ or in $\mathbb{Z}/5\mathbb{Z}$; so there are no solutions in (a,b,c).

In (d), if we start with $\alpha_0 = 2$, a root of X^2+X+1 in $\mathbb{Z}/7\mathbb{Z}$, then successive iterations of Newton's method give subsequent approximate roots in $\mathbb{Q}_7$:

$$\alpha_1 = 2 + 4{\cdot}7 + 5{\cdot}7^2 + 2{\cdot}7^3 + 7^4 + 4{\cdot}7^5 + 5{\cdot}7^6 + 2{\cdot}7^7 + \cdots;$$
$$\alpha_2 = 2 + 4{\cdot}7 + 6{\cdot}7^2 + 3{\cdot}7^3 + 3{\cdot}7^4 + 0{\cdot}7^5 + 4{\cdot}7^6 + 4{\cdot}7^7 + \cdots;$$
$$\alpha_3 = 2 + 4{\cdot}7 + 6{\cdot}7^2 + 3{\cdot}7^3 + 0{\cdot}7^4 + 2{\cdot}7^5 + 6{\cdot}7^6 + 2{\cdot}7^7 + \cdots;$$
$$\alpha_4 = 2 + 4{\cdot}7 + 6{\cdot}7^2 + 3{\cdot}7^3 + 0{\cdot}7^4 + 2{\cdot}7^5 + 6{\cdot}7^6 + 2{\cdot}7^7 + \cdots$$

using the iteration $\alpha_{i+1} = g(\alpha_i)$, $g(\alpha) = \alpha - \frac{\alpha^2+\alpha+1}{2\alpha+1}$. From the last iteration, we obtain an approximate root

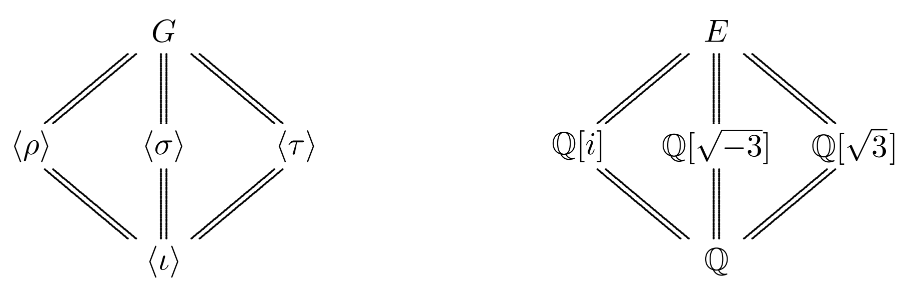
$$2 + 4{\cdot}7 + 6{\cdot}7^2 + 3{\cdot}7^3 + 0{\cdot}7^4 = 1353,$$

correct to within $7^{-5} < 0.00006$. Since the sum of the two roots is -1, the other root is approximately -1354, also correct to the same accuracy. (The second root can be rewritten in standard form as $7^5 - 1354 = 15453 = 4 + 2{\cdot}7 + 0{\cdot}7^2 + 3{\cdot}7^3 + 6{\cdot}7^4$, again correct to within 7^{-5}.)

5. Writing $\zeta = e^{\pi i/6} = \cos\frac{\pi}{6} + i\sin\frac{\pi}{6} = \frac{1}{2}(i+\sqrt{3})$, it is easy to check that ζ is a root of $f(x) = x^4 - x^2 + 1$. Similarly, each of $\zeta, \zeta^5, \zeta^7, \zeta^{11}$ is a root of $f(x)$ so

$$f(x) = x^4 - x^2 + 1 = (x-\zeta)(x-\zeta^5)(x-\zeta^7)(x-\zeta^{11}).$$

Denote the splitting field of this polynomial by $E = \mathbb{Q}(\zeta, \zeta^5, \zeta^7, \zeta^{11}) = \mathbb{Q}(\zeta)$. Note that E contains $\zeta + \zeta^{11} = 2\cos\frac{\pi}{6} = \sqrt{3}$. Since $\zeta \notin \mathbb{R}$ and $\sqrt{3}$ is real irrational, we have proper containments $E \supset \mathbb{Q}[\sqrt{3}] \supset \mathbb{Q}$ and so $[E:\mathbb{Q}] = \big[E:\mathbb{Q}[\sqrt{3}]\big]\big[\mathbb{Q}[\sqrt{3}]:\mathbb{Q}\big] \geqslant 4$. On the other hand, $[E:\mathbb{Q}] \leqslant 4$ since $E = \mathbb{Q}[\zeta]$ where ζ is a root of the polynomial $f(x) \in \mathbb{Z}[x]$ of degree 4. Thus $[E:\mathbb{Q}] = 4$ and $f(x)$ is the minimal polynomial of ζ over $\mathbb{Q}$. Moreover since E is the splitting field of $f(x)$ over $\mathbb{Q}$, the extension $E \supset \mathbb{Q}$ is Galois and its Galois group G has order 4. We may write $G = \{\iota, \rho, \sigma, \tau\}$ where $\rho(\zeta) = \zeta^5$, $\sigma(\zeta) = \zeta^7$ and $\tau(\zeta) = \zeta^{11}$ and $\iota(\zeta) = \zeta$. Note that $\rho^2(\zeta) = \zeta^{25} = \zeta$, $\sigma^2(\zeta) = \zeta^{49} = \zeta$ and $\tau^2(\zeta) = \zeta^{121} = \zeta$ so $\rho^2 = \sigma^2 = \tau^2 = \iota$, i.e. G is a Klein 4-group. Also note that $\rho(\sigma(\zeta)) = \zeta^{35} = \zeta^{11}$ so $\rho\sigma = \tau$. Now ρ fixes $\zeta + \zeta^5 = i$; σ fixes $\zeta{\cdot}\zeta^7 = \zeta^8 = \frac{1}{2}(1 - \sqrt{-3})$; and τ fixes $\zeta + \zeta^{11} = \sqrt{3}$. Each of these last three elements of E is quadratic irrational and therefore generates the fixed field of the corresponding automorphism. Now the subgroups of G and the subfields of E are pictured in the lattice diagrams



where the Galois correspondence is given by $G \leftrightarrow \mathbb{Q}$, $\langle\iota\rangle \leftrightarrow E$, $\langle\rho\rangle \leftrightarrow \mathbb{Q}[i]$, $\langle\sigma\rangle \leftrightarrow \mathbb{Q}[\sqrt{-3}]$, $\langle\tau\rangle \leftrightarrow \mathbb{Q}[\sqrt{3}]$. (I have used double lines to indicate normality.)

6. There was a misprint in the hint given for this problem (the formula for b_j did not appear correctly). The actual question was however stated correctly; and the exact form of the b_j was not important in the solution, only the fact that $b_j \in \mathcal{O}$). In any

case, I have chosen a different presentation here to highlight an interesting generalization of Taylor expansion, made possible by replacing ordinary derivatives by Hasse derivatives. (Recall that the familiar form of Taylor expansion requires denominators $k!$ which are not permitted in prime characteristic.) Also in the online copy of the homework assignment, I rewrote the hint accordingly.

Given $f(X) = \sum_{i=0}^{d} a_i X^i \in F[X]$ and $k \geqslant 0$, the kth *Hasse derivative* of $f(X)$ is the polynomial

$$f^{[k]}(X) = \sum_{i=0}^{d-k} \binom{k+i}{i} a_{k+i} X^i \in F[X].$$

Observe the following:

(i) If $f(X) \in \mathcal{O}[X]$ then $f^{[k]}(X) \in \mathcal{O}[X]$.

(ii) The usual k-th derivative satisfies

$$f^{(k)}(X) = k!f^{[k]}(X) = \sum_{i=0}^{d-k} (i+1)(i+2)\cdots(i+k)a_{k+i}X^i.$$

If F has characteristic zero then we can solve for $f^{[k]}(X) = \frac{1}{k!}f^{(k)}(X)$; however if $p = \operatorname{char} F$ is prime then $f^{(k)}(X) = 0$ whenever $k \geqslant p$ and so $f^{[k]}(X)$ cannot be recovered from $f^{(k)}(X)$; in general the polynomial $f^{[k]}(X)$ contains *more information* not found in the usual derivatives.

(iii) For $k = 1$, our modified 'derivative' coincides with the usual derivative, using the argument in (ii): $f^{[1]}(X) = f^{(1)}(X) = f'(X) = \sum_{i=0}^{d-1}(i+1)a_{i+1}X^i$.

(iv) We easily obtain the identity

$$f(X+\delta) = f(X) + \delta f'(X) + \delta^2 f^{[2]}(X) + \delta^3 f^{[3]}(X) + \cdots + \delta^d f^{[d]}(X)$$

by using the Binomial Theorem to expand each term of $f(X+\delta) = \sum_i a_i(X+\delta)^i$. This identity easily generalizes to more general series $f(X) \in F[[X]]$, giving a more general form of Taylor expansion valid in arbitrary characteristic.

Now suppose $f(X) \in \mathcal{O}[X]$, and $\alpha_0 \in \mathcal{O}$ satisfies $\|f(\alpha_0)\| < \|f'(\alpha_0)\|^2$. We will recursively define the sequence of approximate roots

$$\alpha_{n+1} = \alpha_n + \delta_n \quad \text{where } \delta_n = -\frac{f(\alpha_n)}{f'(\alpha_n)}$$

for $n \geqslant 0$. The first step in this recursion uses $\delta = \delta_0 = -\frac{f(\alpha_0)}{f'(\alpha_0)}$. (Our hypothesis guarantees that $\|f'(\alpha_0)\| > 0$ so that δ is well-defined.) Note that

$$\|\delta\| = \frac{\|f(\alpha_0)\|}{\|f'(\alpha_0)\|} = \frac{\|f(\alpha_0)\|}{\|f'(\alpha_0)\|^2}\|f'(\alpha_0)\| < \|f'(\alpha_0)\| \leqslant 1$$

using the hypothesis $\|f(\alpha_0)\| < \|f'(\alpha_0)\|^2$ and $f'(\alpha_0) \in \mathcal{O}[\alpha_0] \subseteq \mathcal{O}$. In particular, $\alpha_1 = \alpha_0 + \delta \in \mathcal{O}$. By (iv),

$$f(\alpha_1) \;=\; f(\alpha_0{+}\delta) \;=\; f(\alpha_0) + \delta f'(\alpha_0) + \delta^2\varepsilon \;=\; \delta^2\varepsilon$$

where $\varepsilon \in \mathcal{O}$, so

$$\|f(\alpha_1)\| \leqslant \|\delta\|^2 = \frac{\|f(\alpha_0)\|^2}{\|f'(\alpha_0)\|^2}\,.$$

In particular $\|f(\alpha_1)\| = \frac{\|f(\alpha_0)\|}{\|f'(\alpha_0)\|^2}\|f(\alpha_0)\| < \|f(\alpha_0)\|$ which gives (a). Before we can proceed inductively, we first apply (iv) to the polynomial $f'(X) \in \mathcal{O}[X]$ (in place of $f(X)$) to observe that

$$f'(\alpha_1) = f'(\alpha_0{+}\delta) = f'(\alpha_0){+}\delta\tilde{\varepsilon}$$

for some $\tilde{\varepsilon} \in \mathcal{O}$, where

$$\|\delta\tilde{\varepsilon}\| \;\leqslant\; \|\delta\| \;=\; \tfrac{\|f(\alpha_0)\|}{\|f'(\alpha_0)\|^2}\|f'(\alpha_0)\| \;<\; \|f'(\alpha_0)\|$$

so the ultranorm inequality gives

$$\|f'(\alpha_1)\| \;=\; \|f'(\alpha_0) + \delta\tilde{\varepsilon}\| \;=\; \|f'(\alpha_0)\|.$$

Now putting together three of the relations above,

$$\|f'(\alpha_1)\| \;\leqslant\; \frac{\|f(\alpha_0)\|^2}{\|f'(\alpha_0)\|^2} \;<\; \frac{\|f'(\alpha_0)\|^4}{\|f'(\alpha_0)\|^2} \;=\; \|f'(\alpha_0)\|^2 \;=\; \|f'(\alpha_1)\|^2.$$

Thus α_1 satisfies all the same assumptions made for α_0. We may iterate the map $\alpha_n \mapsto \alpha_{n+1}$ and inductively apply the results above at every step. In particular we have $\|f'(\alpha_n)\| = \cdots = \|f'(\alpha_1)\| = \|f'(\alpha_0)\|$ and

$$\|f(\alpha_{n+1})\| \;\leqslant\; \|\delta_n\|^2 \;=\; \frac{\|f(\alpha_n)\|^2}{\|f'(\alpha_n)\|^2} \;=\; \frac{\|f(\alpha_n)\|^2}{\|f'(\alpha_0)\|^2}$$

which establishes (b).

Now let $c = \|f'(\alpha_0)\|$ and $k = \|f(\alpha_0)\|/c^2$. Recall that $\|f'(\alpha_n)\| = c > 0$ for all n; also $k < 1$. An easy induction shows that

(†) $\qquad \|f(\alpha_n)\| \leqslant c^2k^{2^n} \quad$ for all $n \geqslant 0$.

Indeed, $\|f(\alpha_0)\| = c^2k^2$ giving equality for $n = 0$; and assuming (†) holds at iteration n, then as we have seen,

$$\|f(\alpha_{n+1})\| \;\leqslant\; \frac{\|f(\alpha_n)\|^2}{c^2} \;\leqslant\; \frac{(c^2k^{2^n})^2}{c^2} \;=\; c^2k^{2^{n+1}}$$

and so (†) holds also at iteration $n+1$. A consequence of (†) is

$$\|\alpha_{n+1} - \alpha_n\| \;=\; \|\delta_n\| \;=\; \frac{\|f(\alpha_n)\|}{\|f'(\alpha_n)\|} \;\leqslant\; \frac{c^2 k^{2^n}}{c} \;=\; ck^{2^n}$$

and so if $m > n \geqslant 0$ then

$$\begin{aligned} \|\alpha_m - \alpha_n\| \;&=\; \|(\alpha_m - \alpha_{m-1}) + (\alpha_{m-1} - \alpha_{m-2}) + \cdots + (\alpha_{n+1} - \alpha_n)\| \\ &\leqslant\; \max\{ck^{2^{m-1}}, ck^{2^{m-2}}, \ldots, ck^{2^n}\} \;=\; ck^{2^n}. \end{aligned}$$

This shows that the sequence $\alpha_0, \alpha_1, \alpha_2, \ldots \in \mathcal{O}$ is Cauchy, verifying (c). Since $\mathcal{O}$ is complete, we have $\alpha = \lim_{n\to\infty} \alpha_n \in \mathcal{O}$. Since $f(X) \in \mathcal{O}[X]$ is a polynomial, it is continuous and $f(\alpha) = \lim_{n\to\infty} f(\alpha_n) = 0$ where this limit follows from (†).

7. (a) Let $\theta = \alpha + \alpha^2$. Then

$$\theta^3 = \alpha^3 + 3\alpha^4 + 3\alpha^5 + \alpha^6 = 2 + 6\alpha + 6\alpha^2 + 4 = 6 + 6\theta$$

so θ is a root of $f(t) = t^3 - 6t - 6 \in \mathbb{Z}[t]$. By Eisenstein's criterion (with either prime 2 or 3), $f(t)$ is irreducible in $\mathbb{Q}[t]$ so it is the minimal polynomial of θ over $\mathbb{Q}$.

(b) Let $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{5}$. With some computational help from Maple, we find that $f(\alpha) = 0$ where

$$f(x) = x^8 - 40x^6 + 352x^4 - 960x^2 + 576 \in \mathbb{Z}[x].$$

To show that $f(x)$ is the minimal polynomial of α over $\mathbb{Q}$, we must show that it is irreducible in $\mathbb{Z}[x]$ (and hence also irreducible in $\mathbb{Q}[x]$).

Here is a silly argument (I say silly because it uses Maple to jump through lots of unnecessary hoops) but it works. Suppose on the contrary that $f(x) = g(x)h(x)$ where each of the factors $g(x), h(x) \in \mathbb{Z}[x]$ is monic of degree $\geqslant 2$. It is easy to see that $f(x) > 0$ for every $x \geqslant 6$ (in fact a little calculus shows that $f(x)$ represents an increasing function on this interval). It follows that both $g(x)$ and $h(x)$ are positive for $x \geqslant 6$. Now $f(11) = 148534489$ is prime, so $\{g(11), h(11)\} = \{1, 148534489\}$. Similarly, $f(m)$ is prime for at least 63 distinct values of m (such values $m = 11, 13, 31, 35, \ldots, 991$ are easily found using Maple). This means that at least one of the polynomials $g(x), h(x)$, say $g(x)$, assumes the value $g(m) = 1$ for at least 32 integer values of $m \geqslant 11$. But this is impossible: since $\deg g(x) \in \{2, 3, 4, 5, 6\}$, $g(x)$ can assume any one value at most 6 times.

Here is a more conventional argument that accomplishes the same goal. Let $E = \mathbb{Q}(\alpha)$. Clearly $E \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. To verify the reverse containment $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \subseteq E$, one routinely checks (using Maple) that

$$\begin{aligned}\sqrt{2} &= \tfrac{1}{576}\big(\alpha^7 - 28\alpha^5 - 56\alpha^3 + 960\alpha\big);\\ \sqrt{3} &= -\tfrac{1}{96}\big(\alpha^7 - 37\alpha^5 + 244\alpha^3 - 360\alpha\big);\\ \sqrt{5} &= \tfrac{1}{576}\big(5\alpha^7 - 194\alpha^5 + 120\alpha^3 - 2544\alpha\big).\end{aligned}$$

(In fact, each of these relations was found by using Maple to solve a system of 8 linear equations in 8 unknown coefficients.) Thus $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = E$. Note that $E = K(\sqrt{5}) \supseteq K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. To save time, I will make use of the fact (which we have previously shown in class) that $K \supset \mathbb{Q}$ is Galois of degree 4. It suffices to show that $\sqrt{5} \notin K$, as this will force $[E : K] = 2$ and $[E : \mathbb{Q}] = 8$, whence α is algebraic of degree 8 over $\mathbb{Q}$ and $f(x)$ is its minimal polynomial. Suppose that, on the contrary, $\sqrt{5} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \in K$ where $a, b, c, d \in \mathbb{Q}$. Recall that K has 4 automorphisms, one of which is a map σ fixing $\sqrt{3}$ and mapping $\sqrt{2} \mapsto -\sqrt{2}$, also $\sqrt{6} \mapsto -\sqrt{6}$. Now $\sigma(\sqrt{5}) = \pm\sqrt{5}$ since these are the only roots of the polynomial $t^2 - 5 \in \mathbb{Z}[x]$, so either

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = \sqrt{5} = \sigma(\sqrt{5}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

or

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = \sqrt{5} = -\sigma(\sqrt{5}) = -a + b\sqrt{2} - c\sqrt{3} + d\sqrt{6}.$$

In the first case, $\sqrt{5} = a + c\sqrt{3}$; in the second case, $\sqrt{5} = b\sqrt{2} + d\sqrt{6}$. Both of these yield contradictions: in the first case we repeat the argument above with a Galois automorphism of $\mathbb{Q}[\sqrt{3}]$ to get $\pm\sqrt{5} = a - c\sqrt{3}$ whence $\sqrt{5} \in \{a, c\sqrt{3}\}$ which is impossible; the second case takes the form $\sqrt{10} = 2b + 2c\sqrt{6} \in \mathbb{Q}[\sqrt{6}]$ leading to a similar contradiction.

Remarks: The latter argument shows the beginning of an inductive proof that if p_n is the nth prime, then $\sqrt{2} + \sqrt{3} + \sqrt{5} + \cdots + \sqrt{p_n}$ is algebraic of degree 2^n over $\mathbb{Q}$. Some shortcuts are possible in our proof above: in particular it is immediate that all our coefficients $a, b, c, d \in \mathbb{Q}$ above are either integers or half-integers, using the integrality of $\sqrt{5}$. However we had not yet discussed algebraic integers at the time when this homework was assigned.

(c) Denote $\alpha = \sin\frac{2\pi}{7}$ and $\zeta = e^{2\pi i/7}$, so that

$$\begin{aligned}0 &= 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6;\\ 2i\alpha &= \zeta - \zeta^{-1};\\ -4\alpha^2 &= \zeta^2 - 2 + \zeta^{-2};\\ 16\alpha^4 &= \zeta^4 - 4\zeta^2 + 6 - 4\zeta^{-2} + \zeta^{-4};\\ -64\alpha^6 &= \zeta^6 - 6\zeta^4 + 15\zeta^2 - 20 + 15\zeta^{-2} - 6\zeta^{-4} + \zeta^{-6}.\end{aligned}$$

Add row 5, plus 7 times row 4, plus 14 times row 3, and subtract row 1; since $\zeta^7 = 1$ this gives

$$-64\alpha^6 + 112\alpha^4 - 56\alpha^2 = -7.$$

Thus α is a root of $f(x) = 64x^6 - 112x^4 + 56x^2 - 7 \in \mathbb{Z}[x]$. By Eisenstein's criterion (using the prime 7), $f(x)$ is irreducible in $\mathbb{Q}[x]$. Thus the minimal polynomial of α over $\mathbb{Q}$ is

$$\tfrac{1}{64} f(x) = x^6 - \tfrac{7}{4}x^4 + \tfrac{7}{8}x^2 - \tfrac{7}{64}\,.$$