Homework 7 Key

15.8.2) We would like to find each $\gamma \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ such that $\mathbb{Q}(\gamma) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Note that

$$4 = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\gamma)] \cdot [\mathbb{Q}(\gamma) : \mathbb{Q}].$$

Since we would like $\mathbb{Q}(\gamma) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, we must have $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\gamma)] = 1$, so $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 4$, so γ has degree 4 over $\mathbb{Q}$. Now let $\gamma = q + a\sqrt{2} + b\sqrt{3} + c\sqrt{6}$ for $q, a, b, c \in \mathbb{Q}$. If at least two of a, b, c are nonzero, say $a = b = 0$, then γ is a root of $f(x) = (x - q)^2 - 6c^2$, and a similar polynomial exists in the cases where $b = c = 0$ or $a = c = 0$. In each case, γ has degree at most 2 over $\mathbb{Q}$, so these choices of γ do not work.

It remains to show that if at most one of a, b, c is 0, then γ has degree 4 over $\mathbb{Q}$. The degree must be $1, 2$, or 4. Degree 1 is impossible since that would imply $\gamma \in \mathbb{Q}$. Now assume for a contradiction that γ has degree 2 over $\mathbb{Q}$. Note that $\deg(\mathbb{Q}(\gamma)) = \deg(\mathbb{Q}(\gamma - q))$ which follows because q is rational, meaning that γ is a root of a polynomial $f(x)$ iff $\gamma - q$ is a root of the polynomial $f(x + q)$ of the same degree. Therefore we let $\gamma' = \gamma - q$. Since $\deg \gamma' = 2$, there are $m, p \in \mathbb{Q}$ with $\gamma'^2 = m\gamma' + p$, but

$$\begin{aligned}\gamma'^2 &= (a\sqrt{2} + b\sqrt{3} + c\sqrt{6})^2 \\ &= (2a^2 + 3b^2 + 6c^2) + 6bc\sqrt{2} + 4ac\sqrt{3} + 2ab\sqrt{6}.\end{aligned}$$

By our assumption this is equal to

$$p + ma\sqrt{2} + mb\sqrt{3} + mc\sqrt{6}.$$

If $m = 0$, then $ab = ac = bc = 0$, so at least 2 of a, b, c are 0, a contradiction, so $m \neq 0$. Then $6bc = ma$, so $a = \frac{6bc}{m}$. Since $4ac = mb$, we get $\frac{24bc^2}{m} = mb$. If $b, c \neq 0$, then we get $24 = \left(\frac{m}{c}\right)^2$, a contradiction since $\sqrt{24}$ is irrational. Using the other equations, if we assume $a, b \neq 0$ or $a, c \neq 0$, we reach similar contradictions. Since some two of a, b, c must be nonzero, we get a contradiction in any case, so γ' does not have degree 2, so γ does not have degree 2. We conclude that γ has degree 4, and we are done.

15.10.1) Let $A \subset \mathbb{C}$ be the set of all algebraic numbers. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in A[x]$ and let $\alpha \in \mathbb{C}$ be a root of f. Then α is algebraic over $K := \mathbb{Q}(a_0, \ldots, a_n)$, so $[K(\alpha) : K] < \infty$. Then $[K(\alpha) : \mathbb{Q}] = [K(\alpha) : K] \cdot [K : \mathbb{Q}]$, and since the right side is finite, the left side is as well. Thus α is in a finite extension of $\mathbb{Q}$, so α is algebraic over $\mathbb{Q}$, meaning $\alpha \in A$. We conclude that A is algebraically closed.

15.M.1) Let α be transcendental over F, let $K = F(\alpha)$, and let $\beta \in K \setminus F$. Then $\beta = \frac{f(\alpha)}{g(\alpha)}$, where $f, g \in \mathbb{F}[x]$ are not both constant, and f, g are coprime. Then α is a root of the polynomial $f - \beta g \in F(\beta)[x]$, because

$$f(\alpha) - \beta g(\alpha) = f(\alpha) - \frac{f(\alpha)}{g(\alpha)} g(\alpha) = 0.$$

Moreover, $f - \beta g$ is not constant since $f, g \in F[x]$ with g nonzero and $\beta \notin F$. Thus α is algebraic over $F(\beta)$.

4) Let K be a field and let $f \in K[x]$ be a monic polynomial of degree n. Let $K \subset L$ be a splitting field for f, i.e., an extension of the form $K(a_1, \ldots, a_n)$ with

$$f(x) = (x - a_1) \cdots (x - a_n).$$

We prove that $[L : K] \mid n!$ by strong induction on n:

- Base Case: When $n = 1$, f is linear, so $f = x - a_1$, and we must have $a_1 \in K$. Then $L = K(a_1) = K$, so $[L : K] = 1 \mid 1!$.
- Now assume that for a fixed n, any polynomial in $K[x]$ with degree $m \leq n$ has a splitting field F with $[F : K] \mid m!$, and let f have degree $n + 1$. Let $L = K(a_1, \ldots, a_{n+1})$ be a splitting field for f. We have two cases:
  - Case 1: f is irreducible in K. Let a_1 be one of the roots of f. Then $[K(a_1) : K] = n + 1$ since f has degree $n + 1$, so

    $$[L : K] = [L : K(a_1)] \cdot [K(a_1) : K] = (n + 1)[L : K(a_1)].$$

    Now $f = g(x - a_1)$ for some $g \in K(a_1)[x]$ with degree n with splitting field $K(a_1)(a_2, \ldots, a_{n+1})$, which is precisely L, so by the induction hypothesis, $[L : K(a_1)] \mid n!$. Then

    $$[L : K] = (n + 1)[L : K(a_1)] \mid (n + 1)n! = (n + 1)!.$$

  - Case 2: f is reducible in K. Let $f = gh$ with neither of g, h constant. Let $G \subset L$ be the splitting field for g over K, so L is the splitting field for h over G. Let $a := \deg g \leq n$ and $b := \deg h \leq n$. Then by the induction hypothesis, $[G : K] \mid a!$ and $[L : G] \mid b!$. Notice that $a+b = n+1$, and $(a+b)! = a!b!\binom{a+b}{a}$, so

    $$[L : K] = [L : G] \cdot [G : K] \mid a!b! \mid (a + b)! = (n + 1)!,$$

    so $[L : K] \mid (n + 1)!$.

  By strong induction we are done.

5) Let F be a field of characteristic p and let $F \subset K$ be a finite field extension such that p does not divide $[K : F]$. Note that K is separable iff the minimal polynomial f for α is separable for each $\alpha \in K$, which holds iff $f' \neq 0$ for each such f.

Let $\alpha \in K$. Let f be the minimal polynomial of α, so f has degree $n := [F(\alpha) : F] \geq 1$. Since $p \nmid [K : F] = [K : F(\alpha)] \cdot [F(\alpha) : F] = n[K : F(\alpha)]$, it is also the case that $p \nmid n$. But since f is degree n and monic, the coefficient of x^{n-1} for f' is n, and since $n \nmid p$, n is nonzero, so $f' \neq 0$. Thus f is separable, and we conclude that K is a separable field extension of F.

6) Let $f : \mathbb{R} \to \mathbb{R}$ be a field automorphism.

(a) We prove this in steps:

- By definition, $f(0) = 0$ and $f(1) = 1$.
- For any integer $n \geq 1$,

$$f(n) = f(1 + \cdots + 1) = f(1) + \cdots + f(1) = 1 + \cdots + 1 = n.$$

- For $\frac{n}{m}$ with $n, m > 0$ both integers, we have

$$mf\left(\frac{n}{m}\right) = f\left(\frac{n}{m}\right) + \cdots + f\left(\frac{n}{m}\right) = f\left(\frac{n}{m} + \cdots + \frac{n}{m}\right) = f(n) = n,$$

  from which we conclude $f\left(\frac{n}{m}\right) = \frac{n}{m}$.
- We have $0 = f(0) = f(1-1) = f(1) + f(-1) = 1 + f(-1)$, so $f(-1) = -1$. For $q \in \mathbb{Q}$ with $q < 0$, we have $-q > 0$, so $f(q) = f(-1 \cdot -q) = f(-1)f(-q) = -1 \cdot (-q) = q$.

We conclude that $f(q) = q$ for all $q \in \mathbb{Q}$.

(b) If $x > 0$, then $\sqrt{x} \in \mathbb{R}$ is positive as well. So $f(x) = f((\sqrt{x})^2) = f(\sqrt{x})^2 > 0$. We now prove that f is increasing: If $x > y$, then $x - y > 0$, so $f(x - y) = f(x) - f(y) > 0$, so $f(x) > f(y)$.

(c) Assume that $|x - y| < \frac{1}{n}$ for some $n \geq 1$. Then $-\frac{1}{n} < x - y < \frac{1}{n}$, so by parts (a) and (b), $\frac{1}{n} < f(x) - f(y) < \frac{1}{n}$, so $|f(x) - f(y)| < \frac{1}{n}$.

Now let $\varepsilon > 0$. Let $n \in \mathbb{N}$ be large enough so that $\frac{1}{n} < \varepsilon$. Choose $\delta = \frac{1}{n}$. If $|x - y| < \delta = \frac{1}{n}$, then by the above, $|f(x) - f(y)| < \frac{1}{n} < \varepsilon$. Thus f is continuous.

(d) Since the rationals are dense in the reals, and since f is continuous with $f(x) = x$ for all $x \in \mathbb{Q}$, it must be the case that $f(x) = x$ for all $x \in \mathbb{R}$.