ANSWERS TO SOME OF THE HOMEWORK PROBLEMS

Fifth problem set

1. For example, 1 is also a root, hence $x-1$ divides x^2+3x+2. Using long division (since $x-1$ is monic), we find that $x^2+3x+2=(x-1)(x+4)=(x-1)(x-2)$, giving a different factorization.

2. Clearly $\sqrt{2} \equiv -6 \bmod I$, i.e. $\sqrt{2}+I=-6+I$, and hence, for all $a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, $a+b\sqrt{2} \equiv a-6b \bmod I$, i.e. $a+b\sqrt{2}+I=a-6b+I$. Thus the homomorphism $f\colon \mathbb{Z} \to \mathbb{Z}[\sqrt{2}]/I$ is surjective, with kernel $\mathbb{Z}\cap I$. As $34=(6-\sqrt{2})(6+\sqrt{2}) \in \mathbb{Z}\cap I$, $34\mathbb{Z} \subseteq \mathbb{Z}\cap I$. Conversely, if $(a+b\sqrt{2})(6+\sqrt{2}) \in \mathbb{Z}\cap I$, then writing

$$(a+b\sqrt{2})(6+\sqrt{2})=(6a+2b)+(6b+a)\sqrt{2},$$

we see that $a=-6b$ and hence that $6a+2b=-34b \in 34\mathbb{Z}$. Thus $\mathbb{Z}\cap I \subseteq 34\mathbb{Z}$, and hence $\mathbb{Z}\cap I=34\mathbb{Z}$. It follows that $\mathbb{Z}[\sqrt{2}]/I \cong \mathbb{Z}/34\mathbb{Z}$. Since $\mathbb{Z}/34\mathbb{Z}$ is not an integral domain, I is not prime and hence not maximal.

3. (i) By the corollary to long division with remainder, the function $f\colon F \to F[x]/I$ defined by $f(a)=a+I$ is a bijection. (You could also see this directly since every $f(x)$ is of the form $(x-r)g(x)+f(r)$.) The function f is a homomorphism since it is the composition $\pi \circ i$, where $i\colon F \to F[x]$ is the inclusion and $\pi\colon F[x] \to F[x]/I$ is the quotient homomorphism. (Note that the composition $\mathrm{ev}_r \circ i$ is the identity, so that in fact the composition $F \to F[x] \to F[x]/I \to F$ is just the identity.) Since F is a field, I is a maximal and hence a prime ideal
(ii) First part again by long division with remainder, or directly since clearly every $f(x)$ is uniquely of the form $a_0+a_1x+x^2g(x)$. Addition: $(a_0+a_1\alpha)+(b_0+b_1\alpha)=(a_0+b_0)+(a_1+b_1)\alpha$. Multiplication: using $\alpha^2=0$, $(a_0+a_1\alpha)(b_0+b_1\alpha)=a_0b_0+(a_1b_0+a_0b_1)\alpha$. I is not prime, since $\alpha \in F[x]/I$ is a nonzero nilpotent element, and thus $F[x]/I$ is not an integral domain. Of course, you can also see this directly since $x^2=x\cdot x \in I$ but $x \notin I$. Hence I is not maximal.
(iii) First part by long division with remainder. Addition: $(a_0+a_1\alpha)+(b_0+b_1\alpha)=(a_0+b_0)+(a_1+b_1)\alpha$. Multiplication: using $\alpha^2=1$, $(a_0+a_1\alpha)(b_0+b_1\alpha)=(a_0b_0+a_1b_1)+(a_1b_0+a_0b_1)\alpha$. By the above formulas (or directly from $\alpha^2=1$) we see that $(1+\alpha)(1-\alpha)=0$. $F[x]/I$ is not an integral domain, since $1+\alpha$ and $1-\alpha$ are zero divisors; note that they are both

nonzero by the uniqueness statement in the first part of (iii). (They could however be the same element, which happens exactly when $\operatorname{char} F = 2$.) Thus the ideal I is not prime, and so I is not maximal.

(iv) First, $(\mathrm{ev}_1, \mathrm{ev}_{-1})$ is easily seen to be a homomorphism from $F[x]$ to $F \times F$. (Use the fact that each component is a homomorphism.) Clearly $\operatorname{Ker}(\mathrm{ev}_1, \mathrm{ev}_{-1}) = \operatorname{Ker} \mathrm{ev}_1 \cap \operatorname{Ker} \mathrm{ev}_{-1}$. Also, $x^2 - 1 \in \operatorname{Ker} \mathrm{ev}_1 \cap \operatorname{Ker} \mathrm{ev}_{-1}$, and hence $I \subseteq \operatorname{Ker} \mathrm{ev}_1 \cap \operatorname{Ker} \mathrm{ev}_{-1}$. Thus the function $\varphi\colon F[x]/I \to F \times F$ is well-defined. Clearly $\varphi(\alpha) = (\mathrm{ev}_1, \mathrm{ev}_{-1})(x) = (1, -1)$. Hence $\varphi(a + b\alpha) = (a + b, a - b)$ (it is instructive to check directly that with this explicit definition φ is a homomorphism). In particular $\varphi(\frac{1}{2} + \frac{1}{2}\alpha) = (1, 0)$ and $\varphi(\frac{1}{2} - \frac{1}{2}\alpha) = (0, 1)$. (Note that we needed to assume that $\operatorname{char} F \neq 2$ in order to divide by 2.) Hence $\varphi(\frac{1}{2}(a + b) + \frac{1}{2}(a - b)\alpha) = (a, b)$, so that φ is surjective.

(The fact that φ is an isomorphism when $\operatorname{char} F \neq 2$ follows from the Chinese Remainder Theorem. You can check directly that φ is injective, since $\varphi(a + b\alpha) = (a + b, a - b) = (0, 0) \iff a = -b = b$, and again using $\operatorname{char} F \neq 2$ we find that $2b = 0$, hence $a = b = 0$. Another way to see that φ is injective is to check that $\operatorname{Ker} \mathrm{ev}_1 \cap \operatorname{Ker} \mathrm{ev}_{-1} = I$. We have seen that $I \subseteq \operatorname{Ker} \mathrm{ev}_1 \cap \operatorname{Ker} \mathrm{ev}_{-1}$. Conversely, suppose that $g \in \operatorname{Ker} \mathrm{ev}_1 \cap \operatorname{Ker} \mathrm{ev}_{-1}$. Then $\mathrm{ev}_1(g(x)) = 0$, so that $g(x) = (x - 1)h(x)$ for some $h(x) \in F[x]$. But also $\mathrm{ev}_{-1}(g(x)) = 0$, so that $g(-1) = (-1 - 1)h(-1) = -2h(-1) = 0$. Since $\operatorname{char} F \neq 2$, $h(-1) = 0$, so $h(x) = (x + 1)q(x)$ for some $q \in F[x]$. But then $g(x) = (x-1)(x+1)q(x) = (x^2-1)q(x)$, so by definition $g \in (x^2 - 1)$. Hence $\operatorname{Ker} \mathrm{ev}_1 \cap \operatorname{Ker} \mathrm{ev}_{-1} \subseteq I$, and so $\operatorname{Ker} \mathrm{ev}_1 \cap \operatorname{Ker} \mathrm{ev}_{-1} = I$.)

4. If F is infinite and $f \in \operatorname{Ker} \varphi$, then $f(a) = 0$ for all $a \in F$. Since a nonzero polynomial has at most finitely many zeroes, this is only possible if $f = 0$. Hence $\operatorname{Ker} \varphi = \{0\}$, i.e. φ is injective. To find a function $f\colon F \to F$ which is not in the image of φ, it suffices to find a nonzero function which has infinitely many zeroes. For example, fix an element $a \in F$, and define $f\colon F \to F$ via: $f(a) = 1$, and $f(b) = 0$ if $b \neq a$. The the zeroes of f are the set $F - \{a\}$, which is infinite since F is infinite.

If F is finite, say $F = \{a_1, \dots, a_n\}$, then φ cannot be injective just by counting, since $F[x]$ is infinite but F^F is finite. For an explicit example of a nonzero element in $\operatorname{Ker} \varphi$, you can just take $f(x) = (x - a_1) \cdots (x - a_n)$, where as above $F = \{a_1, \dots, a_n\}$. To see that φ is surjective, note that a function $f\colon F \to F$ is specified by its values $f(a_i) = c_i$, say. If we can find a polynomial p_i such that $p_i(a_i) = 1$ and $p_i(a_j) = 0$ for $j \neq i$, consider the polynomial $p = \sum_{i=1}^{n} c_i p_i$. Then $\varphi(p)(a_i) = c_i$ for every i, so that φ is surjective. To find the polynomials p_i, define

$$p_i(x) = A_i \prod_{j \neq i}(x - a_j) \text{ with } A_i = \left(\prod_{j \neq i}(a_i - a_j)\right)^{-1}.$$

Then clearly $p_i(a_j) = 0$ for $j \neq i$ and $p_i(a_i) = 1$.

(Comment: this argument in fact shows that, for F finite with $\#(F) = n$, every function from F to F can be **uniquely** written as a polynomial of degree at most $n-1$, or is zero. In other words, if $F[x]_{\leq n-1}$ is the F-vector space of polynomials with coefficients in F of degree $\leq n-1$ or zero, then φ defines an F-linear isomorphism of additive groups, hence F-vector spaces, from $F[x]_{\leq n-1}$ to F^F—but it is not multiplicative! In fact, you can use this idea to give a nonconstructive proof of the surjectivity of φ.)

Sixth problem set

1. If $\delta = a + b\sqrt{2}$, then $\delta^2 = a^2 + 2b^2 + 2ab\sqrt{2}$. Hence $\delta^2 \in \mathbb{Q} \iff$ either a or b is 0. If $b = 0$, then $\delta^2 = a^2$ is the square of a rational number. If $a = 0$, then $\delta^2 = 2b^2$ where b is a rational number. If $3 = a^2$, then $3 = p^2/q^2$ for positive integers p, q, where we may assume p and q are relatively prime. Thus $p^2 = 3q^2$, hence $3|p^2 \implies 3|p \implies 3^2|p^2 \implies 3|q^2 \implies 3|q$, contradicting the assumption that p and q were relatively prime. A similar argument works if $3 = 2b^2$.

2. By direct computation $(\alpha - \sqrt{2})^2 = 3 = \alpha^2 - 2\sqrt{2}\alpha + 2$. hence $(\alpha^2 - 1)^2 = (-2\sqrt{2}\alpha)^2 = 8\alpha^2$, so that $\alpha^4 - 10\alpha^2 + 1 = 0$. By the properties of $\mathrm{irr}(\alpha, \mathbb{Q}, x)$, $\mathrm{irr}(\alpha, \mathbb{Q}, x)$ divides $x^4 - 10x^2 + 1$. Clearly $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, hence $\mathbb{Q}(\alpha) \leq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Conversely, $\alpha^2 = 5 + 6\sqrt{6}$, hence $\sqrt{6} \in \mathbb{Q}(\alpha)$, hence $\sqrt{6}\,\alpha = 2\sqrt{3} + 3\sqrt{2} \in \mathbb{Q}(\alpha)$. Thus $3\alpha - (2\sqrt{3} + 3\sqrt{2}) = \sqrt{3} \in \mathbb{Q}(\alpha)$, so $\sqrt{2} = \alpha - \sqrt{3} \in \mathbb{Q}(\alpha)$ as well. Thus $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \leq \mathbb{Q}(\alpha)$ and hence $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \leq \mathbb{Q}(\alpha)$.

3. Clearly $\alpha^2 = 3 + 2\sqrt{2}$, hence $\alpha^2 - 3 = 2\sqrt{2}$, so

$$(\alpha^2 - 3)^2 = \alpha^4 - 6\alpha^2 + 9 = (2\sqrt{2})^2 = 8.$$

Thus $\alpha^4 - 6\alpha^2 + 1 = 0$ as claimed. Now

$$x^4 - 6x^2 + 1 = (x^2 + ax + b)(x^2 - ax + b) \iff -a^2 + 2b = -6, \quad b^2 = 1.$$

The second equality says $b = \pm 1$ and the first that $a^2 = 6+2b$. Taking $b = 1$ gives $a^2 = 8$, with no rational solution, but taking $b = -1$ gives $a^2 = 4$ with solutions $a = \pm 2$, hence

$$x^4 - 6x^2 + 1 = (x^2 + 2x - 1)(x^2 - 2x - 1).$$

In particular α must be a root of one of the factors (why?). By the quadratic formula, the roots of $x^2 + 2x - 1$ are $-1 \pm \sqrt{2}$ and those of $x^2 - 2x - 1$ are $1 \pm \sqrt{2}$. Squaring these, we see that $(\pm(1 + \sqrt{2}))^2 = 3 + 2\sqrt{2}$, hence the positive square root is $\alpha = 1 + \sqrt{2}$.

4. We first list all polynomials: Degree 1: x, $x + 1$. Degree 2: x^2, $x^2 + x$, x^2+1, x^2+x+1. Degree 3: x^3, x^3+x^2, x^3+x, x^3+1, x^3+x+1, x^3+x^2+x, $x^3 + x^2 + 1$, $x^3 + x^2 + x + 1$. Irreducible ones: aside from degree 1, where all are irreducible, it suffices to check that neither 0 nor 1 is a root. The first condition says the constant term is 1, not zero; the second, that the number of nonzero monomials is odd. Hence the irreducible polynomials are as follows: Degree 1: x, $x + 1$. Degree 2: $x^2 + x + 1$. Degree 3: $x^3 + x + 1$, $x^3 + x^2 + 1$.

Now, to see if $x^4 + x^3 + x^2 + x + 1$ is irreducible, note that it has no root. So it could only factor as a product of two irreducible quadratic polynomials. But since there is a unique irreducible quadratic polynomial, the only possibility would be that it factors as $(x^2 + x + 1)^2$ (note that over $\mathbb{F}_2$, all nonzero polynomials are monic, so two polynomials which differ by a unit are in fact equal). But (using the fact that the characteristic is 2)

$$(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq x^4 + x^3 + x^2 + x + 1.$$

Hence $x^4 + x^3 + x^2 + x + 1$ is irreducible.

5. Following the discussion, define $\rho(h(x)) = (h(x) + (f(x)), h(x) + (g(x)))$.
(i) We must show that $\operatorname{Ker}\rho = (f(x)g(x))$. First, $h(x) \in \operatorname{Ker}\rho \iff h(x) \in (f(x))$ and $h(x) \in (g(x)) \iff f(x)$ divides $h(x)$ and $g(x)$ divides $h(x)$. Clearly, if $h(x) \in (f(x)g(x))$, then both $f(x)$ and $g(x)$ divide $h(x)$. Conversely, suppose that both $f(x)$ and $g(x)$ divide $h(x)$. Then $h(x) = f(x)p(x)$ for some $p(x) \in F[x]$ and $g(x)$ divides $h(x) = f(x)p(x)$. Since $g(x)$ and $f(x)$ are relatively prime, $g(x)$ divides $p(x)$, say $p(x) = g(x)q(x)$. Then $h(x) = f(x)g(x)q(x)$. Thus $h(x) \in (f(x)g(x))$.
(ii) Suppose that $r(x), s(x)$ are such that $r(x)f(x) + s(x)g(x) = 1$, and set

$$h(x) = r(x)b(x)f(x) + s(x)a(x)g(x).$$

We must show that $h(x) + (f(x))) = a(x) + (f(x)))$ and $h(x) + (g(x))) = b(x) + (g(x)))$. But

$$\begin{aligned} h(x) &\equiv s(x)a(x)g(x) \bmod I; \\ s(x)g(x) &\equiv 1 \bmod I. \end{aligned}$$

Hence $h(x) \equiv a(x) \bmod I$, i.e. $h(x) + (f(x))) = a(x) + (f(x)))$. The proof that $h(x) + (g(x))) = b(x) + (g(x)))$ is similar.

6. By inspection or long division, the other root of $x^2 + x + 1$ is $\alpha + 1$, since

$$(\alpha + 1)^2 + (\alpha + 1) + 1 = \alpha^2 + 1 + \alpha + 1 + 1 = \alpha^2 + \alpha + 1 = 0.$$

Thus $x^2 + x + 1 = (x + \alpha)(x + \alpha + 1)$. A repeated root is not possible, since $(x + \alpha)^2 = x^2 + \alpha^2 = x^2 + \alpha + 1 \neq x^2 + x + 1$.

7. $f(x)$ is irreducible as it has no root ($f(0) = 1$, $f(1) = f(2) = 2$). Since $(\pm\alpha)^2 = -1 = 2$, and $\alpha \neq -\alpha$ as the characteristic is not 2, the factorization of $f(x)$ in $E[x]$ is: $f(x) = (x - \alpha)(x + \alpha) = (x - \alpha)(x - 2\alpha)$. As an abelian group, $E = \{a_0 + a_1\alpha : a_0, a_1 \in \mathbb{F}_3\}$, hence has 9 elements, and the function $f(a_0 + a_1\alpha) = (a_0, a_1)$ defines an isomorphism of additive groups $(E, +) \to (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$. Since E^* has 8 elements and it is cyclic as it is the multiplicative group of a finite field, there are $\varphi(8) = 4$ generators of E^*. As noted, 1 and $2 = -1$ will not work, nor will $\pm\alpha$ since $(\pm\alpha)^2 = -1$, hence $\pm\alpha$ has order 4. This leaves the remaining 4 elements of E^*, namely $\pm(\alpha + 1), \pm(\alpha + 2)$, all 4 of which must then be generators. For example, $(\pm(\alpha+1))^2 = \alpha^2+2\alpha+1 = 2\alpha = -\alpha$ (recall that $\alpha^2+1 = 0$ by construction). Thus $\pm(\alpha+1)$ has order 8, and you can easily check that it generates directly: for example, using $\alpha + 1$, we get

$$\alpha + 1, (\alpha + 1)^2 = 2\alpha, (\alpha + 1)^3 = 2\alpha(\alpha + 1) = 2\alpha + 1, (\alpha + 1)^4 = (2\alpha)^2 = -1,$$

and then $(\alpha + 1)^{4+k} = -(\alpha + 1)^k = 2(\alpha + 1)^k$, giving

$$(\alpha + 1)^5 = 2\alpha + 2, (\alpha + 1)^6 = \alpha, (\alpha + 1)^7 = \alpha + 2, (\alpha + 1)^8 = 1.$$

The other cases $-(\alpha + 1)$ and $\pm(\alpha + 2)$ are similar.

Seventh problem set

1. First we claim that $\sqrt{7} \notin \mathbb{Q}(\sqrt{5})$: if $(a + b\sqrt{5})^2 = a^2 + 5b^2 + 2ab\sqrt{5} = 7$, then $ab = 0$, hence either a or b is 0, hence either $a^2 = 7$ or $5b^2 = 7$. In the first case, writing $a = r/s$ where $r, s \in \mathbb{Z}$ and are relatively prime, we have

$r^2 = 7s^2$, hence $7|r^2$, hence $7|r$ and $7^2|r^2$, but then $7|s^2$ and hence $7|s$, contradicting the fact that r and s were chosen to be relatively prime. A similar argument rules out the possibility that $5b^2 = 7$. Thus $\mathrm{irr}(\sqrt{7}, \mathbb{Q}(\sqrt{5}), x)$ has degree greater than one, and clearly $\mathrm{irr}(\sqrt{7}, \mathbb{Q}(\sqrt{5}), x)$ divides $x^2 - 7$, so that $\mathrm{irr}(\sqrt{7}, \mathbb{Q}(\sqrt{5}), x) = x^2 - 7$, Then $[\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{5})] = 2$, and hence

$$[\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

A basis for $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ as a $\mathbb{Q}$-vector space is then $1, \sqrt{5}, \sqrt{7}, \sqrt{35}$.

With $\alpha = 2\sqrt{5} - \sqrt{7}$,

$$\alpha^2 = 20 + 7 - 4\sqrt{35} = 27 - 4\sqrt{35}.$$

Hence $\sqrt{35} \in \mathbb{Q}(\alpha)$, as is $\sqrt{35}\alpha = 10\sqrt{7} - 7\sqrt{5}$. Thus $10\alpha + (10\sqrt{7} - 7\sqrt{5}) = 23\sqrt{5} \in \mathbb{Q}(\alpha)$, so that $\sqrt{5} \in \mathbb{Q}(\alpha)$ and hence $\sqrt{7} = 2\sqrt{5} - \alpha \in \mathbb{Q}(\alpha)$. It follows that $\mathbb{Q}(\sqrt{5}, \sqrt{7}) \leq \mathbb{Q}(\alpha)$ and hence that $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\alpha)$. Thus $\deg_{\mathbb{Q}} \alpha = 4$. A second basis for $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ as a $\mathbb{Q}$-vector space is then $1, \alpha, \alpha^2, \alpha^3$. Finally,

$$(\alpha^2 - 27)^2 = 16 \cdot 35,$$

and hence $\mathrm{irr}(\alpha, \mathbb{Q}, x) = x^4 - 54x^2 + 169$.

2. Assume that $x^4 - 2$ is irreducible over $\mathbb{Q}$ and hence that $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. (We will have various ways of seeing this later.) Since $\mathbb{Q}(\sqrt[4]{2}) \leq \mathbb{R}$, $i \notin \mathbb{Q}(\sqrt[4]{2}$ and hence $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$ since $\mathrm{irr}(i, \mathbb{Q}(\sqrt[4]{2}), x)$ divides $x^2 + 1$. Thus $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 2 \cdot 4 = 8$, A basis is given by

$$1, \sqrt[4]{2}, (\sqrt[4]{2})^2 = \sqrt{2}, (\sqrt[4]{2})^3, i, i\sqrt[4]{2}, i\sqrt{2}, i(\sqrt[4]{2})^3.$$

As for $\alpha = i + \sqrt[4]{2}$, begin with

$$(\alpha - i)^4 = \alpha^4 - 4i\alpha^3 + 6(-1)\alpha^2 - 4(-i)\alpha + 1 = 2.$$

Then

$$(\alpha^4 - 6\alpha^2 - 1)^2 = [i(4\alpha^3 - 4\alpha)]^2,$$

and expanding out and replacing α by x gives the desired degree 8 polynomial.

(Comment: a somewhat clumsy direct argument shows that $x^4 - 2$ is irreducible over $\mathbb{Q}$, so that $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. Since $\sqrt[4]{2}$ is irrational, $x^4 - 2$ does not have a root in $\mathbb{Q}$ and hence does not have a linear factor in $\mathbb{Q}[x]$, so the only way it could factor over $\mathbb{Q}$ is as a product of two irreducible quadratic polynomials. However, by direct calculation

$$x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2}) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}).$$

Direct inspection shows that no product of two of the four possible factors has rational coefficients: for example, $(x-\sqrt[4]{2})(x+\sqrt[4]{2}) = x^2-\sqrt{2})$, and

$$(x-\sqrt[4]{2})(x\pm i\sqrt[4]{2}) = x^2-(\sqrt[4]{2}\mp i\sqrt[4]{2})x \mp i\sqrt{2},$$

and similarly for the remaining possibilities.)

3. Since $[E:F]=2\neq 1$, $E\neq F$, and hence there exists a $\beta\in E$, $\beta\notin F$. Choosing any such β, we get

$$2=[E:F]=[E:F(\beta)][F(\beta):F],$$

and since $[F(\beta):F]>1$ and divides 2, the only possibility is $[F(\beta):F]=2$ and hence $[E:F(\beta)]=1$, i.e. $E=F(\beta)$. Then $\mathrm{irr}(\beta,F,x)$ has degree 2, say $\mathrm{irr}(\beta,F,x)=x^2+bx+c$, so that $\beta^2+b\beta+c=0$. (Note that it is **not** necessarily true that $\beta^2\in F$.) Under the assumption that $\operatorname{char} F\neq 2$, we can then complete the square:

$$0=\beta^2+b\beta+c=\left(\beta+\frac{b}{2}\right)^2+\left(c-\frac{b^2}{4}\right).$$

Thus, if we set $a=(b^2-4c)/4$ and $\alpha=\beta+b/2$, then $\alpha^2=a$. Since α and β differ by the element $b/2\in F$, $F(\alpha)=F(\beta)$ and $\alpha=\sqrt{a}$ as desired.

4. Let $r\in R$, $r\neq 0$. Since R is a finite-dimensional F-vector space, the sequence of elements $1,r,r^2,\dots,$ is not linearly independent, hence there exists an $n\in\mathbb{N}$ and $a_0,\dots,a_n\in F$, not all 0, such that $\sum_{i=0}^n a_ir^i=0$. Let k be the smallest element of $\{0,\dots,n\}$ such that $a_k\neq 0$. Then

$$0=a_kr^k+\cdots+a_nr^n=r^k(a_k+\cdots+a_nr^{n-k}).$$

Since R is an integral domain and $r\neq 0$, $r^k\neq 0$, and hence $a_k+a_{k+1}r+a_{k+2}r^2\cdots+a_nr^{n-k}=0$. In particular, note that $k=n$ is impossible, hence $n>k$. Rewrite the above as

$$a_k+r(a_{k+1}+a_{k+2}r+\cdots+a_nr^{n-k-1})=0.$$

Solving, we see that

$$1=r(-a_{k+1}a_k^{-1}-a_{k+2}a_k^{-1}r-\cdots-a_na_k^{-1}r^{n-k-1}),$$

and hence r has a multiplicative inverse. Thus R is a field.

5. Since $[E : F] = t > 1$, $E \neq F$, and hence there exists an $\alpha \in E$, $\alpha \notin F$. Choosing any such α, we get

$$t = [E : F] = [E : F(\alpha)][F(\alpha) : F],$$

and since $[F(\alpha) : F] > 1$ and divides t, which is prime, the only possibility is $[F(\alpha) : F] = t$ and hence $[E : F(\alpha)] = 1$, i.e. $E = F(\alpha)$.

6. Suppose that $E = F(\alpha)$ and that $[F(\alpha) : F]$ is odd. If $E \neq F$, i.e. if $\alpha \notin F$, then $[F(\alpha) : F] > 1$. Since $\alpha^2 \in F(\alpha)$, $F \leq F(\alpha^2) \leq F(\alpha)$. Moreover, α is clearly a root of the polynomial $x^2 - \alpha^2$, which has coefficients in $F(\alpha^2)$. Thus $\operatorname{irr}(\alpha, F(\alpha^2), x)$ divides $x^2 - \alpha^2$, and hence $\deg \operatorname{irr}(\alpha, F(\alpha^2), x)$ is either 1 or 2. Note that $\deg \operatorname{irr}(\alpha, F(\alpha^2), x) = [F(\alpha) : F(\alpha^2)]$. But $\deg \operatorname{irr}(\alpha, F(\alpha^2), x) = 2$ is impossible, since in that case $2 = [F(\alpha) : F(\alpha^2)]$ divides $[F(\alpha) : F]$, which is odd, a contradiction. Hence

$$\deg \operatorname{irr}(\alpha, F(\alpha^2), x) = [F(\alpha) : F(\alpha^2)] = 1,$$

so that $F(\alpha^2) = F(\alpha)$.

7. Clearly β is algebraic over $F(\alpha)$ since it is a root of $\operatorname{irr}(\beta, F, x) \in F[x] \subseteq (F(\alpha))[x]$. Moreover $\operatorname{irr}(\beta, F(\alpha), x)$ divides $\operatorname{irr}(\beta, F, x)$, and hence $\deg_{F(\alpha)} \beta \leq m$. Thus $[F(\alpha, \beta) : F(\alpha)] = \deg_{F(\alpha)} \beta \leq m$. By considering the sequence of extensions

$$F \leq F(\alpha) \leq F(\alpha, \beta),$$

we see that

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F] = [F(\alpha, \beta) : F(\alpha)] \cdot n \leq mn.$$

The remaining statements are clear.

8. By the previous problem, $[F(\alpha, \beta) : F] \leq mn$. Again using the fact that $[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F]$, it follows that n divides $[F(\alpha, \beta) : F]$. By symmetry, m also divides $[F(\alpha, \beta) : F]$. Since n and m are relatively prime, nm, which is the least common multiple of n and m, divides $[F(\alpha, \beta) : F]$. But since $[F(\alpha, \beta) : F] \leq nm$, we must have $[F(\alpha, \beta) : F] = nm$. In particular $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$.