Exercise (2.1).

Proof. Suppose K is a degree two extension of $\mathbb{Q}$. Then, pick any $x \in K \setminus \mathbb{Q}$. We have that $\mathbb{Q} \subseteq \mathbb{Q}(x) \subseteq K$, but $[\mathbb{Q}(x) : \mathbb{Q}] \neq 1$, so $\mathbb{Q}(x) = K$. So, K is obtained by adding a root of a (monic) degree two polynomial to $\mathbb{Q}$. If this polynomial is $t^2 + ax + b$, then completing the square gives the polynomial

$$(t - a/2)^2 + b - a^2/4$$

and so $K = \mathbb{Q}(\sqrt{b - a^2/4})$. Clearing denominators, we have that $K = \mathbb{Q}(\sqrt{m})$, where $b - a^2/4 = m/n^2$ for some $n \in \mathbb{Z}$.

Now, suppose $m, n \in \mathbb{Z}$ are squarefree (and not equal to 1). If $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{n})$, then there are $a, b \in \mathbb{Q}$ with $\sqrt{n} = a + b\sqrt{m}$. Squaring gives

$$n = a^2 + mb^2 + 2ab\sqrt{m}$$

By unique representations in $\mathbb{Q}(\sqrt{m})$, we must therefore have $n = a^2 + mb^2$ and $2ab = 0$. If $b = 0$, then this is a contradiction, since we get $n = a^2$, but n is squarefree. So, $b \neq 0$, and so $a = 0$, which gives $n = mb^2$. Since n is squarefree, we must thus have $b = \pm 1$, and so $n = m$. In other words, the fields $\mathbb{Q}(\sqrt{n})$ are distinct for n squarefree. □

Exercise (2.2).

Proof. Let $R = \mathbb{Z}[\sqrt{-3}]$. It is clear that $I \neq 2R$, since $1 + \sqrt{3} \in I$, but $\frac{1+\sqrt{-3}}{2} \notin R$. On the other hand, we have:

$$I^2 = (2, 1 + \sqrt{-3})^2 = (4, 2 + 2\sqrt{-3}, -2 + 2\sqrt{-3}) = (4, 2 + 2\sqrt{-3}) = 2(2, 1 + \sqrt{-3}) = 2I$$

as claimed. Thus, ideals in R don't factorize uniquely into primes, since the ideal I^2 would have the two distinct factorizations coming from doubling the exponents on the prime factors of I and the factorization coming from concatenating the factorizations of I and $2R$.

For the rest of the statement, we first show that I is prime. Indeed,

$$R/I = \mathbb{Z}[\sqrt{-3}]/(2, 1 + \sqrt{-3}) = \mathbb{Z}[x]/(2, 1 + x, x^2 + 3) = \mathbb{F}_2[x]/(x + 1, x^2 + 3) = \mathbb{F}_2$$

is a domain. In fact it is a field, so I is maximal.

Second, suppose that P is a prime ideal containing $2R$. Then it necessarily contained 2, and also,

$$(1 + \sqrt{-3})^2 = -2 + 2\sqrt{-3} \in 2R$$

hence $1 + \sqrt{-3} \in P$ since P is prime. So, P contains I, but since I is maximal we get $P = I$.

Third, note that a product of ideals is necessarily contained in each of the multiplicands. So, if $2R$ has a factorization, each factor must contain $2R$, and so a factorization into primes must be of the form $2R = I^k$ since this is the only prime containing $2R$ as we've just shown. We also know $k \geq 2$ since $2R \neq R$ and we've shown $2R \neq I$. But then we have:

$$I^3 \subseteq I^2 = 2I = I^{k+1} \subseteq I^3$$

and so all of these ideals are equal, which we need to show cannot be. But,

$$I^3 = (I^2)I = (2I)I = 4I$$

and so in particular $4 \in 2I = I^2$, but $4 \notin 4I = I^3$. Hence $I^3 \neq I^2$. □

Exercise (2.3).

Proof. To finish the proof, we need to show that for $r, s \in \mathbb{Q}$ and m squarefree such that $2r$ and $r^2 - ms^2$ are integers, if $m \equiv 2, 3 \pmod 4$:

$$r, s \in \mathbb{Z}$$

and otherwise for $m \equiv 1 \pmod 4$:

$$2r, 2s \in \mathbb{Z} \text{ and } 2r \equiv 2s \pmod 2$$

Since $2r \in \mathbb{Z}$, we consider the two cases of it being even and odd. If $2r$ is even, then $r \in \mathbb{Z}$. Then $ms^2 \in \mathbb{Z}$ as well, and since m is squarefree, this gives that $s^2 \in \mathbb{Z}$, and hence $s \in \mathbb{Z}$. This can happen in either case for m above.

Otherwise $2r$ is odd. Then $4ms^2 = (2r)^2 - 4(r^2 - ms^2)$ is an integer. As before, since m is squarefree, we conclude $4s^2$ is an integer, and so $2s \in \mathbb{Z}$ as well. Furthermore, the expression above is the difference of an odd square and a multiple of four, so we get $m(2s)^2 \equiv 1 \pmod 4$. Hence we get that $2s$ is odd and $m \equiv 1 \pmod 4$. This falls under the second case. □

Exercise (2.4).

Proof. The proof of theorem 2 shows a more general fact: if $A \subseteq B$ are rings, then an element $\alpha \in B$ is integral over A (in that it satisfies a monic polynomial with coefficients in A) iff $A[\alpha]$ is a finite A-module iff $\alpha \in C$ for some A-subalgebra C of B that is a finite A-module. So, since $a_0, \ldots, a_{n-1}$ are algebraic integers, we have that each of the extensions:

$$\mathbb{Z} \subseteq \mathbb{Z}[a_0] \subseteq \mathbb{Z}[a_0, a_1] \subseteq \cdots \subseteq \mathbb{Z}[a_0, \ldots, a_{n-1}]$$

are finite extensions of modules. Further, since α is integral over this final extension, we also have that $\mathbb{Z}[a_0, \ldots, a_{n-1}] \subseteq \mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$ is a finite extension. Hence, by our tower laws, $\mathbb{Z} \subseteq \mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$ is a finite extension of modules. This is a $\mathbb{Z}$-subalgebra of, say, $\mathbb{C}$ that contains α, and so α is integral over $\mathbb{Z}$, i.e. it is an algebraic integer. □

Exercise (2.5).

Proof. Note that for $a \in \mathbb{F}_p$, $a^p = a$, and for any two elements α, β in a ring of characteristic p, $(\alpha + \beta)^p = \alpha^p + \beta^p$. By induction, this latter fact extends to arbitrary finite sums. Hence, if $f \in \mathbb{F}_p[x]$, then,

$$(f(x))^p = \left(\sum_{i=0}^{n} a_i x^i\right)^p = \sum_{i=0}^{n} (a_i x^i)^p = \sum_{i=0}^{n} a_i (x^p)^i = f(x^p)$$

as claimed. □

Exercise (2.6).

Proof. Since $f^2 \mid g$, we have $g = f^2 h$ for some $h \in K[x]$. Then, differentiating gives

$$g' = 2ff'h + f^2 h' = f(2f'h + fh')$$

which is clearly divisible by f. □

Exercise (2.7).

Proof. For $k \in (\mathbb{Z}/m\mathbb{Z})^\times$, we have an automorphism of $\mathbb{Q}[\omega]$ that maps ω to ω^k. If we have two such automorphisms, corresponding to k and ℓ, then under the composition:

$$\omega \mapsto \omega^k \mapsto (\omega^\ell)^k = \omega^{kl}$$

where the exponent can, of course, be considered modulo m. Hence composition of automorphisms corresponds to multiplication in $(\mathbb{Z}/m\mathbb{Z})^\times$. □

Exercise (2.8)**.**

(a) Let $\omega = e^{2\pi i/p}$, p an odd prime. Show that $\mathbb{Q}[\omega]$ contains $\sqrt{p}$ if $p \equiv 1 \pmod 4$, and $\sqrt{-p}$ if $p \equiv -1 \pmod 4$. Express $\sqrt{-3}$ and $\sqrt{5}$ as polynomials in the appropriate ω.

(b) Show that the 8th cyclotomic field contains $\sqrt{2}$.

(c) Show that every quadratic field is contained in a cyclotomic field.

Proof.

(a) First, here's a very unmotivated explicit solution (skip below the line for the "better" proof). Let $\chi(n)$ denote the Legendre symbol, so that χ depends only on the residue mod p, $\chi(0) = 0$ and otherwise $\chi(n) = 1$ if and only if n is a perfect square mod p. For $t \in \{1, \ldots, p-1\}$, let t^{-1} denote the unique integer in $\{1, \ldots, p-1\}$ such that tt^{-1} is 1 modulo p. Define

$$a_r = \sum_{n=1}^{p-1} \chi(n(r-n))$$

Note that:

$$a_0 = \sum_{n=1}^{p-1} \chi(-n^2) = \chi(-1)(p-1)$$

and for $1 \leq r \leq p-1$,

$$a_r = \sum_{n=1}^{p-1} \chi((r^{-1})^2)\chi(n(r-n)) = \sum_{n=1}^{p-1} \chi(r^{-1}n(1-r^{-1}n)) = \sum_{k=1}^{p-1} \chi(k(1-k)) = a_1$$

since multiplication by r^{-1} simply permutes $\{1, \ldots, p-1\}$. Finally, define

$$f(x) = \sum_{n=0}^{p-1} \chi(n)x^n$$

If γ satisfies $\gamma^p = 1$, then

$$\begin{aligned}
(f(\gamma))^2 &= \left(\sum_{n=0}^{p-1} \chi(n)\gamma^n\right)^2 \\
&= \sum_{n=0}^{p-1}\sum_{m=0}^{p-1} \chi(n)\chi(m)\gamma^{n+m} \\
&= \sum_{r=0}^{p-1}\sum_{m=0}^{p-1} \chi(m(r-m))\gamma^r && \text{for } r \equiv n+m \\
&= \sum_{r=0}^{p-1} a_r\gamma^r \\
&= \chi(-1)(p-1) + a_1\sum_{r=1}^{p-1}\gamma^r
\end{aligned}$$

On one hand, since $1^p = 1$, we can take $\gamma = 1$. But $f(1) = 0$ since there are exactly $(p-1)/2$ residues and nonresidues modulo p. So, this gives

$$\chi(-1)(p-1) + (p-1)a_1 = 0 \implies a_1 = -\chi(-1)$$

On the other hand, we can take $\gamma = \omega$ which gives:

$$f(\omega)^2 = \chi(-1)(p-1) + a_1\sum_{r=1}^{p-1}\omega^r = \chi(-1)(p-1) + \chi(-1) = \chi(-1)p$$

which is what we wished to show, since now $f(\omega)$ is in $\mathbb{Q}(\omega)$ and has square $\pm p$.

"Better" proof: We've shown that $\operatorname{disc}(\omega) = p^{p-2}$ if $p \equiv 1 \pmod 4$ and $\operatorname{disc}(\omega) = -p^{p-2}$ otherwise. But we can write $\operatorname{disc}(\omega) = |\sigma_i(\omega^j)|^2$, where $|\cdot|$ denotes the determinant, and i, j range over the appropriate indices. Thus, $\pm p^{p-2}$ is a square of an element in $\mathbb{Q}[\omega]$, and since p is odd, so is p^{p-3}. Hence, the quotient is a square in $\mathbb{Q}[\omega]$, namely $\sqrt{\pm p} \in \mathbb{Q}[\omega]$.

Now, we consider the explicit cases. Note that the "worse" proof actually helps here, since it was very explicit. For $p = 3$, the proof showed that

$$\sqrt{-3} = \omega - \omega^2 = \omega - \omega^{-1}$$

which is also clear since $\omega^{\pm 1} = -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$. For $p = 5$, the proof showed:

$$\sqrt{5} = \omega - \omega^2 - \omega^3 + \omega^4$$

To confirm this, we can square the expression:

$$(\omega - \omega^2 - \omega^3 + \omega^4)^2 = \omega^2 - 2\omega^3 - \omega^4 + 4\omega^5 - \omega^6 - 2\omega^7 + \omega^8 = 4 - \omega - \omega^2 - \omega^3 - \omega^4 = 5$$

as claimed.

(b) Let $\omega = e^{2\pi i/8}$. Then, $\omega^2 = i$, so:

$$(\omega + \omega^{-1})^2 = \omega^2 + 2 + \omega^{-2} = i + 2 - i = 2$$

i.e. $\sqrt{2} = \pm(\omega + \omega^{-1}) \in \mathbb{Q}[\omega]$.

(c) Let m be squarefree. Then we can write m as a product of primes $\pm p_1 \cdots p_k$. Consider the field $K = \mathbb{Q}(\omega)$, where $\omega = e^{2\pi i/(8m)}$. Then, $\omega^m = \sqrt{i}$, so K contains the 8th cyclotomic field, and so contains $\sqrt{2}$. Similarly, $\omega^{2m} = i$, and so K contains $\sqrt{-1}$. Finally, for each odd prime divisor p_j, $\omega^{4m/p_j} = e^{2\pi i/p_j}$, so K contains $\sqrt{\pm p_j}$ for each j. Hence, multiplying the necessary terms, we have that K contains $\sqrt{m}$. □

Exercise (2.9).

Proof. Let $\zeta_j = e^{2\pi i/j}$. As suggested, suppose $\omega = \zeta_m$ and that θ is a primitive kth root of unity, so that $\theta = e^{2\pi ih/k} = \zeta_k^h$ for some h with $(h,k) = 1$. Then, we can write $ah + bk = 1$ for some $a, b \in \mathbb{Z}$. Second, if $d = (m,k)$ is the gcd, then there are t, v such that $tm + vk = d$. Let $u = at$. Finally, since r is the lcm of m and k, we have $r = mk/d$. So,

$$\theta^u \omega^v = \theta^{at}\omega^v = \zeta_k^{hat}\zeta_m^v = \zeta_k^{(1-bk)t}\zeta_m^v = \zeta_k^t\zeta_m^v = \zeta_{rd/m}^t\zeta_{rd/k}^v = \zeta_r^{tm/d}\zeta_r^{vk/d} = \zeta_r^{(tm+vk)/d} = \zeta_r$$

as claimed. □

Exercise (2.10).

Proof. We'll proceed by induction on m. As a base case, suppose that m is a power of two, i.e. $m = 2^a$ for some $a \geq 1$ (since m is even). Then we can write $r = 2^b r'$ for some r' odd and $b \geq a$. Thus, we get:

$$2^{a-1} = \phi(m) \geq \phi(r) = 2^{b-1}\phi(r')$$

which gives $a = b$ and $\phi(r') = 1$, so $r' = 1$, since r' is odd. I.e. $r = 2^a = m$ as claimed.

Otherwise, m has an odd prime divisor p. Similar to above, write $m = p^a m'$ and $r = p^b r'$ for $a \leq b$ and m', r' not divisible by p. Then,

$$\phi(m') = \frac{\phi(m)}{\phi(p^a)} \geq \frac{\phi(r)}{\phi(p^b)} = \phi(r')$$

since ϕ is multiplicative and $\phi(p^j) = p^{j-1}(p-1)$ is increasing in j. But m' is even and $m' \mid r'$, so by induction, we have $m' = r'$. Finally, we have

$$p^{a-1}(p-1) = \phi(p^a) = \frac{\phi(m)}{\phi(m')} \geq \frac{\phi(r)}{\phi(r')} = \phi(p^b) = p^{b-1}(p-1)$$

so $a \geq b$, i.e. $a = b$. So, $r = m$ and we're done. □

Exercise (2.11).

Proof. Factorize f: $f(x) = \prod_{i=1}^n (x - a_i)$. Then, the coefficient of x_r is

$$\sum_S \prod_{i \in S} (-a_i)$$

where S ranges over all subsets of $\{1, \ldots, n\}$ with $|S| = r$. So, the magnitude of the coefficient is at most

$$\left| \sum_S \prod_{i \in S} (-a_i) \right| \leq \sum_S \prod_{i \in S} |a_i| = \sum_S 1 = \binom{n}{r}$$

since there are exactly $\binom{n}{r}$ such S.

Second, consider the set T_n of all roots of all polynomials with integer coefficients of degree n such that the coefficient of x^r has magnitude at most $\binom{n}{r}$. Notice this is a finite set, since there are finitely many such polynomials and each one has at most n distinct roots. I claim this contains all described numbers. Indeed, let α be an algebraic integer of degree n all of whose conjugates have magnitude 1. Then, let f be the (monic) minimal polynomial of α. We've seen that f must have integer coefficients since α is an algebraic integer. Then, all roots of f have magnitude 1, since the roots are precisely the conjugates of α. Hence, the computation above shows that $\alpha \in T_n$ since f is one of the described polynomials.

Finally, in this case, note that α^k is also an algebraic integer for all $k \geq 1$, and that $|\sigma_i(\alpha^k)| = |\sigma_i(\alpha)|^k = 1$ for all embeddings σ_i. Finally, $\alpha^k \in \mathbb{Q}(\alpha)$, so α^k has degree at most n. Hence, all of the powers of α are contained in the finite set $T_1 \cup \cdots \cup T_n$, and so by Pigeonhole, we must have $\alpha^j = \alpha^k$ for some $j < k$. I.e. $\alpha^{k-j} = 1$ so α is a root of unity. □

Exercise (2.12).

Proof. First, note that the conjugate of an element of $\mathbb{Z}[\omega]$ is again in $\mathbb{Z}[\omega]$ since $\overline{\omega} = \omega^{-1}$. Hence, if u is a unit in $\mathbb{Z}[\omega]$, we have $v \in \mathbb{Z}[\omega]$ with $uv = 1$, and so $1 = \overline{u} \cdot \overline{v}$ and so $\overline{u}$ is also a unit in $\mathbb{Z}[\omega]$. Hence, $u/\overline{u} \in \mathbb{Z}[\omega]$ is an algebraic integer. Finally, to see that $u/\overline{u}$ is a root of unity, it suffices to show that each conjugate has magnitude 1. But any automorphism of $\mathbb{Q}[\omega]$ commutes with complex conjugation, so if σ is such an automorphism, then:

$$\left|\sigma\left(\frac{u}{\overline{u}}\right)\right| = \left|\frac{\sigma(u)}{\overline{\sigma(u)}}\right| = 1$$

which completes the claim. We've characterized the roots of unity in $\mathbb{Q}[\omega]$ to be precisely the $2p$th roots of unity, since p is odd, which can be written as $\pm\omega^k$ for some $0 \leq k < p$.

Now, suppose for contradiction that $u/\overline{u} = -\omega^k$ for some k. Then, $u^p = (-\overline{u}\omega^k)^p = -\overline{u^p}$. But now, by (1.25), we have that $u^p \equiv a \pmod{p}$ for some $a \in \mathbb{Z}$. Then,

$$a \equiv u^p \equiv -\overline{u^p} \equiv -a \pmod{p}$$

Hence $p \mid 2a$, and so $p \mid a$ since p is an odd prime. So, $p \mid u^p$, i.e. $u^p = p\alpha$ for some $\alpha \in \mathbb{Z}[\omega]$. But u is a unit, so dividing by it gives $1/p \in \mathbb{Z}[\omega]$, which is not true. □

Exercise (2.13).

Proof. As noted, for a number field K and $\alpha \in \mathbb{A} \cap K$, α is a unit if and only if $N(\alpha) = \pm 1$. So, let $m \in \mathbb{Z}$ be squarefree, negative, and neither of $-1, -3$, and let $K = \mathbb{Q}(\sqrt{m})$. Now, writing $\alpha = a + b\sqrt{m}$, we have $N(\alpha) = a^2 - mb^2$. Since $m < 0$, we have that $a^2 - mb^2 \geq 0$, and so if α is a unit, it must have norm $+1$. We now show that b must be zero by casework.

If $m \equiv 1 \pmod{4}$, then we have $m \leq -7$ since we've excluded the case $m = -3$. We also have $a, b \in \frac{1}{2}\mathbb{Z}$ in this case. If $b \neq 0$, then we have $b^2 \geq \frac{1}{4}$, and so $a^2 - mb^2 \geq 0 + \frac{7}{4} > 1$, contrary to assumption. So $b = 0$ in this case.

Otherwise, $m \equiv 2, 3 \pmod{4}$, so $m \leq -2$ and $a, b \in \mathbb{Z}$. Then, if $b \neq 0$ we have $a^2 - mb^2 \geq 2 \cdot 1 > 1$, again contrary to assumption.

So, in either case we have $b = 0$. Then we need $a^2 = 1$, and so $a = \pm 1$ which gives that $\alpha = \pm 1$ are the only possible units. It is also clear that they are both units.

For the case $m = -1$, we have $\mathbb{A} \cap \mathbb{Q}[i] = \mathbb{Z}[i]$ and we've seen that the units are precisely $\pm 1, \pm i$. For the case $m = -3$, we have $\mathbb{A} \cap QQ[\sqrt{-3}] = \mathbb{Z}[\omega]$ for ω a primitive cube root of unity. Then the units are $\pm 1, \pm\omega, \pm\omega^2$. □

Exercise (2.14).

Proof. We have that $1 + \sqrt{2}$ is a unit since

$$(1 + \sqrt{2})(\sqrt{2} - 1) = 2 - 1 = 1$$

But it isn't a root of unity since $1+\sqrt{2}$ is a real number greater than 1, so $(1+\sqrt{2})^n > 1$ for all n. Hence, the elements $(1+\sqrt{2})^n$ are distinct for all n, but they are all elements of $\mathbb{Z}[\sqrt{2}]$. So, there are integers $a_n, b_n \in \mathbb{Z}$ with $(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$. Taking norms, we get:

$$a_n^2 - 2b_n^2 = N((1 + \sqrt{2})^n) = N(1 + \sqrt{2})^n = (-1)^n$$

So, this gives infinitely many solutions to each of $a^2 - 2b^2 = 1$ and $a^2 - 2b^2 = -1$ for integers a, b by taking n even and odd, respectively. □

Exercise (2.15).

Proof. An arbitrary element of $\mathbb{Z}[\sqrt{-5}]$ is of the form $a + b\sqrt{-5}$ and has norm $a^2 + 5b^2$. But there are clearly no integer solutions to $a^2 + 5b^2 = 2, 3$, since such a solution must have $b = 0$, else $a^2 + 5b^2$ would be too large, but then $a = \sqrt{2}, \sqrt{3}$, which are not integers.

Now, to see that $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ is an example of nonunique factorization, it suffices to note that each term is irreducible and that neither $1 \pm \sqrt{-5}$ is divisible by 2 in $\mathbb{Z}[\sqrt{-5}]$. The latter fact is obvious, and to note that the elements are irreducible, we take norms:

$$N(2) = 4 \qquad N(3) = 9 \qquad N(1 \pm \sqrt{-5}) = 6$$

But then if α is a proper irreducible factor of one of these terms, we would get $N(\alpha)$ is a nonunit integer divisor of the corresponding norm. But then $N(\alpha)$ has to be either 2 or 3, which we've seen cannot be. □

Exercise (2.16).

Proof. First, note that $T(\alpha) = \alpha + i\alpha - \alpha - i\alpha = 0$. Similarly, we have $T(\alpha^2), T(\alpha^3) = 0$. So, as suggested by the hint, write $\sqrt{3} = a + b\alpha + c\alpha^2 + d\alpha^3$, and by linearity of the trace, we have $T(\sqrt{3}) = a$. On the other hand, we know that the only conjugates of $\sqrt{3}$ are $\pm\sqrt{3}$, so $T(\sqrt{3}) = 2(\sqrt{3} - \sqrt{3}) = 0$. So, $a = 0$.

Continuing with the hint, consider $\sqrt{3}/\alpha = b + c\alpha + d\alpha^2$. This has trace b. On the other hand, we have precisely four conjugates:

$$\pm\sqrt{3}/\alpha, \pm i\sqrt{3}/\alpha$$

since these are all roots of $2t^4 - 9$, which is irreducible since its reciprocal polynomial $9t^4 - 2$ is irreducible by Eisenstein ($p = 2$). But the sum of these is also zero, so we get $b = 0$.

Similarly, we have $\sqrt{3}/\alpha^2 = c + d\alpha$, and taking traces gives $c = 0$ since the conjugates are $\pm\sqrt{3}/\alpha^2$. Finally, we have $\sqrt{3} = d\alpha^3$, and squaring gives $3 = d^2\alpha^6 = 2d^2\alpha^2$, which contradicts linear independence of 1 and α^2 over $\mathbb{Q}$. □

Exercise (2.17).

Proof. Assume L/K is a finite extension of degree n as usual. Note that $K \subseteq K[\alpha] \subseteq L$ is a tower of fields. Hence, in particular, L is a $K[\alpha]$-vector space, so we can choose a basis $\beta_1, \ldots, \beta_r$. Then, if α is an element of degree d over K (it must be finite since L/K is finite), then it satisfies a polynomial

$$\alpha^d + c_{d-1}\alpha^{d-1} + \cdots + c_0 = 0$$

Then, $1, \alpha, \ldots, \alpha^{d-1}$ is a basis for $K[\alpha]$ over K. Then the $n = dr$ elements $\beta_i\alpha^j$ for $1 \leq i \leq r$ and $0 \leq j < d$ form a basis for L over K. With respect to this basis, multiplication by α is block diagonal, with each block of the form:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & 0 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & 0 & 0 & \cdots & 0 & -c_2 \\ 0 & 0 & 1 & 0 & \cdots & 0 & -c_3 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & -c_{d-2} \\ 0 & 0 & 0 & 0 & \cdots & 1 & -c_{d-1} \end{pmatrix}$$

and a total of r blocks (one for each β_i). Then the trace of this block is $-c_{d-1}$, which is the sum of the roots of the minimal polynomial above of α, i.e. $-c_{d-1} = t(\alpha)$ as denoted in the text. This gives the equality on traces: $T(\alpha) = \frac{n}{d}t(\alpha) = r(-c_{d-1})$, which is the trace of the full block diagonal matrix.

The determinant is similar: the determinant of the above block is $(-1)^d c_0$, which is the product of the roots of the minimal polynomial. In other words, we have $N(\alpha) = (n(\alpha))^{n/d} = \left[(-1)^d c_0\right]^r$, which is the determinant of the full block diagonal matrix. □

Exercise (2.18).

Proof. Suppose that $\sigma_i\tau_j = \sigma_r\tau_s$ pointwise on M. Then, each τ_a fixes L pointwise, so for $\ell \in L$, we have:

$$\sigma_i(\ell) = \sigma_i(\tau_j(\ell)) = \sigma_r(\tau_s(\ell)) = \sigma_r(\ell)$$

So, we must have $i = r$ since σ_i and σ_r act identically on L. In N, we can now compose with the automorphism σ_i^{-1} to get $\tau_j = \tau_s$ on M, which implies $j = s$, as desired. □

Exercise (2.19).

Proof. For the induction, note that if $n = 1$, we have that the determinant of the 1×1 matrix 1 is just 1, which is the product over pairs i, j of $a_i - a_j$ (since it is the empty product).

Now, for the induction step, let

$$A = \begin{pmatrix} 1 & a_1 & \cdots & a_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^{n-1} \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & a_1 & \cdots & a_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^n \\ 1 & a_{n+1} & \cdots & a_{n+1}^n \end{pmatrix}$$

and we assume

$$\det(A) = \prod_{1 \le i < j \le n} (a_i - a_j)$$

Now, consider the polynomial:

$$f(t) = \prod_{i=1}^{n} (t - a_i) = t^n + c_{n-1}t^{n-1} + \cdots + c_0$$

and define

$$C = \begin{pmatrix} 1 & 0 & \cdots & 0 & c_0 \\ 0 & 1 & \cdots & 0 & c_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & c_{n-1} \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

Then, we have $\det(C) = 1$, and so:

$$\begin{aligned} \det(B) &= \det(B)\det(C) \\ &= \det(BC) \\ &= \det \begin{pmatrix} 1 & a_1 & \cdots & a_1^{n-1} & f(a_1) \\ 1 & a_2 & \cdots & a_2^{n-1} & f(a_2) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & a_n & \cdots & a_n^{n-1} & f(a_n) \\ 1 & a_{n+1} & \cdots & a_{n+1}^{n-1} & f(a_{n+1}) \end{pmatrix} \\ &= \det \begin{pmatrix} 1 & a_1 & \cdots & a_1^{n-1} & 0 \\ 1 & a_2 & \cdots & a_2^{n-1} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & a_n & \cdots & a_n^{n-1} & 0 \\ 1 & a_{n+1} & \cdots & a_{n+1}^{n-1} & f(a_{n+1}) \end{pmatrix} \\ &= f(a_{n+1})\det(A) \\ &= \prod_{i=1}^{n} (a_{n+1} - a_i) \cdot \prod_{1 \le i < j \le n} (a_j - a_i) \\ &= \prod_{1 \le i < j \le n+1} (a_j - a_i) \end{aligned}$$

as desired. □

Exercise (2.20).

Proof. First, note that f has no repeated roots. Indeed, if $\beta \in \mathbb{C}$ is a multiple root of f, then $f(x) = (x-\beta)^2 g(x)$ for some $g \in \mathbb{C}[x]$. Then $f'(x) = 2(x-\beta)g(x) + (x-\beta)^2 g'(x)$ has β as a root. In other words, both f and f' are divisible by the minimal polynomial of β in $K[x]$, and since f is irreducible, it must actually equal the minimal polynomial of β. But then $f \mid f'$, which cannot be since $\deg(f') < \deg(f)$.

So, we have that

$$f(x) = \prod_{\beta} (x - \beta)$$

where the product ranges over all roots of f in $\mathbb{C}$. Then,

$$f'(x) = \sum_{\gamma} \prod_{\beta \neq \gamma} (x - \beta)$$

and so

$$f'(\alpha) = \sum_{\gamma} \prod_{\beta \neq \gamma} (\alpha - \beta) = \prod_{\beta \neq \alpha} (\alpha - \beta)$$

as desired. □

Exercise (2.21).

Proof. Let $m \in \mathbb{Z}[x]$ be the minimal polynomial for α. Then, since $f(\alpha) = 0$, we have $m \mid f$, so that $f(x) = m(x)g(x)$ for some polynomial g. By Gauss' Lemma, $g \in \mathbb{Z}[x]$ and is monic. Then,

$$N(f'(\alpha)) = N(m'(\alpha)g(\alpha) + m(\alpha)g'(\alpha)) = N(m'(\alpha)g(\alpha)) = N(m'(\alpha))N(g(\alpha)) = \pm \operatorname{disc}(\alpha)N(g(\alpha))$$

which shows the claim since $N(g(\alpha)) \in \mathbb{Z}$. □

Exercise (2.22).

Proof. Note that

$$P = \sum_{g \in A_n} \prod_{i=1}^{n} \sigma_i(\alpha_{g(i)})$$

where A_n is the alternating group of even permutations. Similarly, N is the same, but with $g \notin A_n$. This makes it clear that P, N are algebraic integers, since ach $\sigma_i(\alpha_j)$ is, and these are in the ring they generate.

Now, fix a normal extension L of K/Q. Let f be an automorphism of L. Then, for each i, $f \circ \sigma_i$ is an embedding of K into $\mathbb{C}$ that fixes $\mathbb{Q}$, so $f \circ \sigma_i = \sigma_{h(i)}$ for some $h(i)$. Then h is a permutation since composing with f^{-1} inverts this association. So,

$$f(P) = \sum_{g \in A_n} \prod_{i=1}^{n} f(\sigma_i(\alpha_{g(i)})) = \sum_{g \in A_n} \prod_{i=1}^{n} \sigma_{h(i)}(\alpha_{g(i)}) = \sum_{g \in A_n} \prod_{i=1}^{n} \sigma_i(\alpha_{(g \circ h^{-1})(i)})$$

Thus, if h is even, then $f(P) = P$ and if h is odd, then $f(P) = N$. Similarly, we find that $f(N) = N$ or $f(N) = P$ in these two cases, respectively.

So, f fixes both $P + N$ and PN. Since f was arbitrary, $P + N$ and PN are fixed by every automorphism of L, so that $P + N$ and PN are in $\mathbb{Q}$. Finally, this gives that they are algebraic integers in $\mathbb{Q}$, so they must be in $\mathbb{Z}$. This gives $d = (P - N)^2 = (P + N)^2 - 4PN$ is either 0 or 1 mod 4. □

Exercise (2.23).

Proof. □

Exercise (2.24).

Proof. As noted, any subgroup of $\mathbb{Z}$ is either trivial or infinite cyclic, and so is free abelian of rank 0 or 1. Now, suppose any subgroup of $\mathbb{Z}^{n-1}$ is free abelian of rank $\leq n - 1$, let $H \subseteq \mathbb{Z}^n$, let $\pi : \mathbb{Z}^n \to \mathbb{Z}$ be projection onto the first coordinate and let $K = \ker(\pi)$. Then $\pi(H)$ is a subgroup of $\mathbb{Z}$, so it is either trivial or infinite cyclic.

If it is trivial, then $H \subseteq K$, so H is free abelian by the inductive hypothesis. Otherwise, choose $h \in H$ with $\pi(h)$ generating the image. Then H is the direct sum of $\langle h \rangle$ and $H \cap K$. Indeed, if $g \in H$, then $\pi(g) \in \pi(H)$, so $\pi(g) = \pi(h^r)$ for some r. Thus $h^{-r}g \in \ker(\pi) = K$ and is clearly in H, so $g = h^r(h^{-r}g)$ is in $\langle h \rangle (H \cap K)$ as desired. Further, nothing is in the intersection since $\pi(h^r)$ is nonzero for all nonzero r. Since $H \cap K$ is a subgroup of K, it is free abelian of rank at most $n - 1$, so this gives that H is free abelian of rank at most n. □

Exercise (2.25).

Proof. Since α is algebraic, it satisfies a polynomial with coefficients in $\mathbb{Z}$ (not necessarily monic) by clearing denominators. I.e.

$$a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$$

for some $a_0, \ldots, a_n \in \mathbb{Z}$ and $a_n \neq 0$. Multiplying through by a_n^{n-1} gives:

$$(a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + a_{n-2}a_n(a_n\alpha)^{n-2} + \cdots + a_n^{n-1}a_0 = 0$$

and this is an integral relation for $a_n\alpha$.

So, if $\{\alpha_1, \ldots, \alpha_k\}$ is a finite set of algebraic numbers, there are integers $m_1, \ldots, m_k$ such that $m_i\alpha_i$ are algebraic integers for all i, whence $m\alpha_i$ is an algebraic integer for all i for $m = m_1 \cdots m_k$. □

Exercise (2.26).

Proof. □

Exercise (2.27).

Proof. □

Exercise (2.28). *Let $f(x) = x^3 + ax + b$, $a, b \in \mathbb{Z}$, and assume f is irreducible over $\mathbb{Q}$. Let α be a root of f.*

(a) Show that $f'(\alpha) = -(2a\alpha + 3b)/\alpha$.

(b) Find $N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(2a\alpha + 3b)$.

(c) Show that $\operatorname{disc}(\alpha) = -(4a^3 + 27b^2)$.

(d) Suppose $\alpha^3 = \alpha + 1$. Prove that $\{1, \alpha, \alpha^2\}$ is an integral basis for the ring of integers in $\mathbb{Q}[\alpha]$. Do the same if $\alpha^3 + \alpha = 1$.

Proof.

(a) We have

$$\alpha f'(\alpha) = \alpha(3\alpha^2 + a) = 3\alpha^3 + a\alpha = 3(-a\alpha - b) + a\alpha = -(2a\alpha + 3b)$$

as claimed.

(b) Now, let $\alpha_1, \alpha_2, \alpha_3$ denote the three roots of f. Then,

$$f(x) = \prod_i (x - \alpha_i)$$

and

$$\begin{aligned} N(2a\alpha + 3b) &= \prod_i (2a\alpha_i + 3b) \\ &= (-2a)^3 \prod_i \left(-\frac{3b}{2a} - \alpha_i \right) \\ &= -8a^3 f\left(-\frac{3b}{2a} \right) \\ &= -8a^3 \left(-\frac{27b^3}{8a^3} - a\frac{3b}{2a} + b \right) \\ &= 27b^3 + 4a^3 b \end{aligned}$$

(c) So, we can compute the discriminant, noting that N is multiplicative and $N(\alpha) = -b$ from the constant term of f:

$$\operatorname{disc}(\alpha) = -N(f'(\alpha)) = -N\left(-\frac{2a\alpha + 3b}{\alpha} \right) = -(-1)^3 \frac{b(27b^2 + 4a^3)}{-b} = -(4a^3 + 27b^2)$$

as claimed.

(d) Finally, we consider the explicit examples. If $\alpha^3 = \alpha + 1$, then

$$\operatorname{disc}(\alpha) = -(4(-1)^3 + 27(-1)^2) = -23$$

This is squarefree, so we get that $\mathbb{Z}[\alpha]$ is the ring of integers in $\mathbb{Q}(\alpha)$. Second, if $\alpha^3 + \alpha = 1$, then

$$\operatorname{disc}(\alpha) = -(4 \cdot 1^3 + 27(-1)^2) = -31$$

which is also squarefree, giving the same result. □

Exercise (2.29).

Proof. In the first case, let $R = \mathbb{Z}[(1 + \sqrt{m})/2]$ and $S = \mathbb{Z}[(1 + \sqrt{n})/2]$, and note these are the rings of integers in each of their fraction fields. Then, $\operatorname{disc}(R) = m$ and $\operatorname{disc}(S) = n$ are coprime, so the ring of integers in $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ is $RS = \mathbb{Z}[(1 + \sqrt{m})/2, (1 + \sqrt{n})/2]$, which has integral basis:

$$1, \frac{1 + \sqrt{m}}{2}, \frac{1 + \sqrt{n}}{2}, \frac{1 + \sqrt{m} + \sqrt{n} + \sqrt{mn}}{4}$$

and discriminant $(mn)^2$ by Exercise 23(c).

In the second case, let $R = \mathbb{Z}[(1+\sqrt{m})/2]$ as before, but let $S = \mathbb{Z}[\sqrt{n}]$ to be the corresponding rings of integers again. Then $\mathrm{disc}(R) = m$ and $\mathrm{disc}(S) = 4n$ are again coprime, so the ring of integers in $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ is RS which has integral basis:

$$1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{1+\sqrt{m}}{2}\sqrt{n}$$

and discriminant $16m^2n^2$. □

Exercise (2.30). *Let $K = \mathbb{Q}[\sqrt{7}, \sqrt{10}]$ and fix any $\alpha \in \mathbb{A} \cap K$. We will show that $\mathbb{A} \cap K \neq \mathbb{Z}[\alpha]$. Let f denote the monic irreducible polynomial for α over $\mathbb{Z}$ and for each $g \in \mathbb{Z}[x]$ let $\overline{g}$ denote the polynomial in $\mathbb{Z}_3[x]$ obtained by reducing coefficients* $(\mathrm{mod}\ 3)$.

(a) Show that $g(\alpha)$ is divisible by 3 in $\mathbb{Z}[\alpha]$ iff $\overline{g}$ is divisible by $\overline{f}$ in $\mathbb{Z}_3[x]$.

(b) Now suppose $\mathbb{Z} \cap K = \mathbb{Z}[\alpha]$. Consider the four algebraic integers

$$\alpha_1 = (1+\sqrt{7})(1+\sqrt{10})$$
$$\alpha_2 = (1+\sqrt{7})(1-\sqrt{10})$$
$$\alpha_3 = (1-\sqrt{7})(1+\sqrt{10})$$
$$\alpha_4 = (1-\sqrt{7})(1-\sqrt{10})$$

Show that all products $\alpha_i\alpha_j$ $(i \neq j)$ are divisible by 3 in $\mathbb{Z}[\alpha]$, but that 3 does not divide any power of any α_i.

(c) Let $\alpha_i = f_i(\alpha)$, $f_i \in \mathbb{Z}[x]$ for each $i = 1, 2, 3, 4$. Show that $\overline{f} \mid \overline{f_i f_j}$ $(i \neq j)$ in $\mathbb{Z}_3[x]$ but $\overline{f} \nmid \overline{f_i}^n$. Conclude that for each i, $\overline{f}$ has an irreducible factor (over $\mathbb{Z}_3$) which does not divide $\overline{f_i}$ but which does divide all $\overline{f_j}$, $j \neq i$.

(d) This shows that $\overline{f}$ has at least four distinct irreducible factors over $\mathbb{Z}_3$. On the other hand f has degree at most 4. Why is that a contradiction?

Proof. We show the first claim. Suppose $g(\alpha)$ is divisible by 3. Then there is some $\beta \in \mathbb{Z}[\alpha]$ with $g(\alpha) = 3\beta$, and $\beta = h(\alpha)$ for some $h \in \mathbb{Z}[x]$. Then α is a root of $g(x) - 3h(x)$, so $f \mid g - 3h$. Reducing mod 3 gives $\overline{f} \mid \overline{g}$ as claimed. Each of these steps is reversible: if $\overline{f} \mid \overline{g}$, then $f \mid g + 3h$ for some h, whence $g(\alpha) + 3h(\alpha) = 0$, i.e. $g(\alpha) = -3h(\alpha)$ is a multiple of 3.

For the second, note that $(1+\sqrt{7})(1-\sqrt{7}) = -6$ and $(1+\sqrt{10})(1-\sqrt{10}) = -9$ are both multiples of 3, so each product $\alpha_i\alpha_j$ is a multiple of 3 since each product consists of at least one of these pairs of terms. On the other hand, we do have that the α_i are a full set of conjugates, so the trace of α_i^n is

$$\alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n$$

On the other hand, we have

$$4^n = (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^n = \alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n + \cdots$$

where the excluded terms, from the binomial theorem, each include the product of two different terms. In other words, each term in the "$\cdots$" is a multiple of 3 in $\mathbb{Z}[\alpha]$, so we can write the trace as $1 + 3\beta$ for some $\beta \in \mathbb{Z}[\alpha]$. By unique representation of numbers in $\mathbb{Q}(\alpha)$, we thus have that $\beta \in \mathbb{Z}$, since the trace is an integer. I.e. the trace is 1 mod 3 and therefore not a multiple of 3. So, α_i^n is not a multiple of 3 in $\mathbb{Z}[\alpha]$.

The next result is immediate by combining these two: for $\alpha_i = f_i(\alpha)$, we have that 3 divides $\alpha_i\alpha_j$, so $\overline{f}$ divides $\overline{f_i f_j}$ in $\mathbb{F}_3[x]$, and 3 does not divide α_i^n, so $\overline{f}$ does not divide $\overline{f_i^n}$. Since $\mathbb{F}_3[x]$ is a UFD (even a PID), we have that this latter statement implies that there is a prime π_i that divides $\overline{f}$ but not $\overline{f_i}$. But then π_i divides $\overline{f_i f_j}$, so it divides $\overline{f_j}$ for all $j \neq i$.

Finally, we have that $\overline{f}$ is divisible by the four (distinct) primes $\pi_1, \ldots, \pi_4$ and hence their product. These cannot all be degree 1, since there are only three degree 1 monic polynomials in $\mathbb{F}_3[x]$: $x, x+1, x+2$. So, at least one has degree 2, whence the product has degree at least $1+1+1+2 = 5$. But f is the minimal polynomial of α, and so has degree 4. This gives the contradiction. Thus the ring of integers is not monogenic. □

Exercise (2.31).

Proof. Let $\alpha = (\sqrt{3}+\sqrt{7})/2$. Then,

$$4\alpha^2 = 10 + 2\sqrt{21}$$

so that:

$$84 = (4\alpha^2 - 10)^2 = 16\alpha^4 - 80\alpha^2 + 100$$

i.e.

$$\alpha^4 - 5\alpha^2 + 1 = 0$$

so that α is an algebraic integer. But α isn't in RS where $R = \mathbb{Z}[\sqrt{3}]$ and $S = \mathbb{Z}[\sqrt{7}]$ are the rings of integers of their respective fraction fields, despite α being in the compositum field. □

Exercise (2.32).

Proof. Let ω be a primitive cube root of unity, and let $\alpha = \sqrt[3]{2}$ be the (real) cube root of two. Then $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\omega\alpha)$ are fields of degree three over $\mathbb{Q}$, while the compositum is $\mathbb{Q}(\alpha, \omega)$ has degree six over $\mathbb{Q}$. □

Exercise (2.33).

Proof. Note that the norm is the product of the conjugates, and that we've determined the conjugates of ω to be precisely ω^k for $1 \leq k \leq m$ coprime to m. But if $(k, m) = 1$, then $(m - k, m) = 1$, and $m - k \neq k$ since otherwise $m = 2k$ and $(k, m) = k = m/2 > 1$. This gives a pairing on the set of conjugates, so we get:

$$N(\omega) = \prod_{\substack{1\leq k\leq m\\(k,m)=1}} = \prod_{\substack{1\leq k<m/2\\(k,m)=1}} \omega^k\omega^{m-k} = 1$$

since each term equals 1. □

Exercise (2.34).

Proof. Let $\alpha = 1 + \omega + \cdots + \omega^{k-1}$. Since m and k are coprime, there are $a, b \in \mathbb{Z}$ with $am + bk = 1$. Then, let

$$\beta = 1 + \omega^k + \omega^{2k} + \cdots + \omega^{(b-1)k}$$

Then,

$$\alpha\beta = \left(\sum_{i=0}^{k-1}\omega^i\right)\left(\sum_{j=0}^{b-1}\omega^{jk}\right) = \sum_{i=0}^{k-1}\sum_{j=0}^{b-1}\omega^{jk+i} = \sum_{n=0}^{bk-1}\omega^n = \frac{1-\omega^{bk}}{1-\omega} = \frac{1-\omega^{1-am}}{1-\omega} = \frac{1-\omega}{1-\omega} = 1$$

for $n = jk + i$ - the ranges for i, j biject via this map onto $n = 0, \ldots, bk - 1$.

For the second half, note that we have

$$p = \prod_{\substack{1\leq k\leq m\\p\nmid k}} (1 - \omega^k)$$

For such a k, we have:

$$(1 + \omega + \cdots + \omega^{k-1})(1 - \omega) = 1 - \omega^k$$

and we've just shown this first factor is a unit. So, $1 - \omega^k = u_k(1 - \omega)$ for a unit u_k for each such k. So,

$$p = \prod_{\substack{1\leq k\leq m\\p\nmid k}} u_k(1 - \omega) = u(1 - \omega)^n$$

where u is the product of the u_k and hence a unit, and $n = \varphi(m)$ is the number of terms in the product. □

Exercise (2.35).

Proof. Since $\omega\theta = \omega^2 + 1$, we have that ω is a root of $x^2 - \theta x + 1$.

Second, note that $\overline{\omega} = \omega^{-1}$, and so $\overline{\theta} = \overline{\omega + \omega^{-1}} = \omega^{-1} + \omega = \theta$, so $\theta \in \mathbb{R}$. Then, we have $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\omega) \cap \mathbb{R} \subseteq \mathbb{Q}(\omega)$, and the last inclusion is proper since $\omega \notin \mathbb{R}$. But the tower has degree at most 2 since ω satisfies a degree 2 polynomial over $\mathbb{Q}(\theta)$, and so we must have the degree is exactly two and the intermediate degrees are 1 and 2, respectively, i.e. $\mathbb{Q}(\theta) = \mathbb{Q}(\omega)\cap\mathbb{R}$.

Note σ has order 2, so the fixed field K has degree 2 as a subfield of $\mathbb{Q}(\omega)$. Further, $\sigma(\theta) = \theta$ as we've already noted, so $\theta \in K$ which gives $\mathbb{Q}(\theta) \subseteq K \subseteq \mathbb{Q}(\omega)$, and the degrees again force $K = \mathbb{Q}(\theta)$.

In one direction, we have:

$$\mathbb{A} \cap \mathbb{Q}[\theta] \subseteq \mathbb{Q}[\theta] \subseteq \mathbb{R} \text{ and } \mathbb{A} \cap \mathbb{Q}[\theta] \subseteq \mathbb{A} \cap \mathbb{Q}[\omega] = \mathbb{Z}[\omega]$$

Conversely:

$$\mathbb{R} \cap \mathbb{Z}[\omega] \subseteq \mathbb{R} \cap \mathbb{Q}[\omega] = \mathbb{Q}[\theta] \text{ and } \mathbb{R} \cap \mathbb{Z}[\omega] \subseteq \mathbb{Z}[\omega] \subseteq \mathbb{A}$$

so the two sets are equal.

More generally, let B be a ring with a subring A such that B is a free A-module, and let $u \in B$ be a unit. Then, if $\{b_i\}$ is a basis for B over A, then $\{b_i u\}$ is also a basis for B over A. Indeed, it spans, for if $b \in B$, then $bu^{-1} \in B$, so there exists $a_i \in A$ with

$$bu^{-1} = \sum_i a_i b_i$$

and multiplying by u gives the result. Further, they are independent, for if

$$\sum_i a_i b_i u = 0$$

then multiplying through by u^{-1} gives a relation on the original basis, whence each a_i is zero.

So, $\{1, \omega, \omega^{-1}, \ldots, \omega^{n-1}, \omega^{1-n}, \omega^n\}$ is an integral basis since it is obtained from the usual basis $\{1, \omega, \ldots, \omega^{2n-1}\}$ by multiplying through by the unit ω^{1-n}.

Finally, to see that $\{1, \omega, \theta, \theta\omega, \ldots, \theta^{n-1}, \theta^{n-1}\omega\}$ is a basis, we want to express each element in terms of the previous basis. Half of the terms are just powers of θ, which can be evaluated:

$$\theta^k = (\omega + \omega^{-1})^k = \sum_{i=0}^{k} \binom{k}{i} \omega^{k-2i}$$

and so this column of the change-of-basis matrix indeed has integer entries, and further, the exponents are in the range $-k, \ldots, k$, so this column has all zeros below the main diagonal. The following column is $\theta^k\omega$, which is given by taking this column and shifting each entry down one position. Hence, the entire matrix has integer entries and is upper triangular. So, the determinant is the product of the diagonal, which is the coefficient of ω^{-k} in θ^k, which is 1 for each term. So, this matrix has determinant 1, showing that this set has the same discriminant (and so is also a basis).

We know that $\mathbb{Z}[\theta] \subseteq \mathbb{Q}(\theta) \cap \mathbb{A}$ since each of these are algebraic integers in this field. We've also shown that $\mathbb{Q}(\theta) \cap \mathbb{A} = \mathbb{Z}[\omega] \cap \mathbb{R}$, and any element of this ring is a $\mathbb{Z}$-linear combination of θ^k and $\theta^k\omega$ for $k = 0, \ldots, n-1$. Let x be such an element, and group terms, so that

$$x = (a_0 + \cdots + a_{n-1}\theta^{n-1}) + \omega(b_0 + \cdots + b_{n-1}\theta^{n-1})$$

for integers a_i, b_i. But if the first parenthesized term is already in $\mathbb{R}$ since $\mathbb{Z}[\theta] \subseteq \mathbb{R}$, so in order for x to be in $\mathbb{Z}[\omega] \cap \mathbb{R}$, we must have that the second term is also real. But it is a real multiple of ω, which can only be real if it is zero. So, we get that

$$x = a_0 + \cdots + a_{n-1}\theta^{n-1} \in \mathbb{Z}[\theta]$$

as claimed.

Finally, we consider $m = p$ for an odd prime p, so that $n = \varphi(m)/2 = (p-1)/2$. Now consider the tower of fields $\mathbb{Q} \subseteq \mathbb{Q}(\theta) \subseteq \mathbb{Q}(\omega)$. Then $1, \theta, \ldots, \theta^{n-1}$ is a basis for $\mathbb{Q}(\theta)$ over $\mathbb{Q}$, and $1, \omega$ is a basis for $\mathbb{Q}(\omega)$ over $\mathbb{Q}(\theta)$. So, by exercise 23, we get:

$$\operatorname{disc}_{\mathbb{Q}}^{\mathbb{Q}(\omega)}(1, \omega, \theta, \theta\omega, \ldots, \theta^{n-1}, \theta^{n-1}\omega) = \left(\operatorname{disc}_{\mathbb{Q}}^{\mathbb{Q}(\theta)}(1, \theta, \ldots, \theta^{n-1})\right)^2 N_{\mathbb{Q}}^{\mathbb{Q}(\theta)} \left(\operatorname{disc}_{\mathbb{Q}(\theta)}^{\mathbb{Q}(\omega)}(1, \omega)\right)$$

The LHS is the discriminant of an integral basis of $\mathbb{Q}(\omega)$, which does not depend on the basis, so we have that it equals $(-1)^n p^{p-2}$. For the final term, we can compute directly. For brevity, let $T = Tr_{\mathbb{Q}(\theta)}^{\mathbb{Q}(\omega)}$. From the constant term of the minimal polynomial $x^2 - \theta x + 1$ of ω over $\mathbb{Q}(\theta)$, we can see that the other conjugate of ω is ω^{-1}. Thus,

$$\operatorname{disc}_{\mathbb{Q}(\theta)}^{\mathbb{Q}(\omega)}(1, \omega) = \det \begin{pmatrix} 1 & \omega \\ 1 & \omega^{-1} \end{pmatrix}^2 = (\omega - \omega^{-1})^2$$

Now we need to take the norm. By transitivity, we have:

$$\begin{aligned} N_{\mathbb{Q}}^{\mathbb{Q}(\omega)}(\omega-\omega^{-1}) &= N_{\mathbb{Q}}^{\mathbb{Q}(\theta)}(N_{\mathbb{Q}(\theta)}^{\mathbb{Q}(\omega)}(\omega-\omega^{-1})) \\ &= N_{\mathbb{Q}}^{\mathbb{Q}(\theta)}((\omega-\omega^{-1})(\omega^{-1}-\omega)) \\ &= N_{\mathbb{Q}}^{\mathbb{Q}(\theta)}(-(\omega-\omega^{-1})^2) \\ &= (-1)^n N_{\mathbb{Q}}^{\mathbb{Q}(\theta)}((\omega-\omega^{-1})^2) \end{aligned}$$

So, it suffices to compute this first norm. Directly, we get:

$$\begin{aligned} N_{\mathbb{Q}}^{\mathbb{Q}(\omega)}(\omega-\omega^{-1}) &= \prod_{i=1}^{p-1}(\omega^i-\omega^{-i}) \\ &= \omega^{\sum_{i=1}^{p-1} i}\prod_{i=1}^{p-1}(1-\omega^{-2i}) \\ &= \omega^{(p-1)p/2}\prod_{i=1}^{p-1}(1-\omega^{-2i}) \\ &= p \end{aligned}$$

since the exponent on ω is a multiple of p, and the product is the evaluation of $(x^p-1)/(x-1)$ at $x=1$, since it has all the primitive pth roots of unity as zeros.

Finally, we combine all of our computations to get:

$$(-1)^n p^{p-2} = \left(\operatorname{disc}_{\mathbb{Q}}^{\mathbb{Q}(\theta)}(1,\theta,\dots,\theta^{n-1})\right)^2 (-1)^n p$$

and so

$$\operatorname{disc}(\theta) = \operatorname{disc}_{\mathbb{Q}}^{\mathbb{Q}(\theta)}(1,\theta,\dots,\theta^{n-1}) = p^{(p-3)/2}$$

as claimed. □

Exercise (2.36).

Proof. First, we show the set spans. Let $\gamma \in R_{k+1}$. Then $\pi(\gamma) \in \pi(R_{k+1})$, so $\pi(\gamma) = a\pi(\beta)$ since $\pi(\beta)$ generates the image. Now, $\pi(\gamma - a\beta) = 0$, so $\gamma - a\beta \in \ker(\pi) \cap R_{k+1}$. But $\ker(\pi) = F_k$, so $\gamma - a\beta \in F_k \cap R_{k+1} \subseteq F_k \cap R = R_k$. The remaining terms in the set form a $\mathbb{Z}$-basis for R_k, so this shows that

$$\gamma = a\beta + \left(a_0 + a_1\frac{f_1(\alpha)}{d_1} + \cdots + a_{k-1}\frac{f_{k-1}(\alpha)}{d_{k-1}}\right)$$

for some $a_i \in \mathbb{Z}$. So it spans.

Further, the set is independent. Indeed, if

$$0 = a\beta + a_0 + \cdots + a_{k-1}\frac{f_{k-1}(\alpha)}{d_{k-1}}$$

Then, applying π gives $0 = a\pi(\beta)$ since each f_i has degree $i < k$. But $\pi(\beta)$ generates the infinite cyclic image, so we must have $a = 0$. Then the relation above becomes a relation on the remaining terms, which were known to be independent. So $a_i = 0$ for each i as well; thus the described set is a basis. □

Exercise (2.37).

Proof. Let $h = f - g$. Then h has degree $< n$ as well, but $h(\alpha) = f(\alpha) - g(\alpha) = 0$. So h cannot be nonzero, else the degree of α would be smaller than n, i.e. $h = 0$, so that $f = g$. □

Exercise (2.38).

Proof. That this set is a basis is clear from the proof. Now, since $d_1 \mid \cdots \mid d_{k-1}$, we have that $d_{k-1}R_k \subseteq \mathbb{Z}[\alpha]$. Conversely, suppose that $mR_k \subseteq \mathbb{Z}[\alpha]$. Then, in particular, $\frac{f_{k-1}(\alpha)}{d_{k-1}} \in R_k$, so $\frac{m}{d_{k-1}}f_{k-1}(\alpha) \in \mathbb{Z}[\alpha]$. Since f_{k-1} has degree $k-1 < n$, and α is an algebraic integer of degree n, we have that the representation given here is unique, i.e. this is an element of $\mathbb{Z}[\alpha]$ iff each coefficient is an integer. Finally, f_{k-1} is monic, so the leading coefficient gives $m/d_{k-1} \in \mathbb{Z}$, i.e. $d_{k-1} \mid m$, so $m \geq d_{k-1}$.

This shows that d_{k-1} is the smallest integer with the desired property. □

Exercise (2.39).

Proof. Since each $g_j(\alpha)/d_j$ is an algebraic integer and the set $\{f_i(\alpha)/d_i\}$ is an integral basis, there is an integer matrix A such that

$$g_j(\alpha)/d_j = \sum_i A_{ij} f_i(\alpha)/d_i$$

It suffices to show $\det A = 1$. But since g_j is monic of degree j, f_i is monic of degree i, and $i, j < n$ are all less than the degree of α, we get that A must be upper triangular with each diagonal element equal to 1. So, $\det A = 1$ as claimed. □

Exercise (2.40).

Proof. It's clear that the f_i form an integral basis for $\mathbb{Z}[\alpha]$. Then,

$$\operatorname{disc}(\alpha) = \operatorname{disc}(1, f_1(\alpha), \dots, f_{n-1}(\alpha)) = (d_1 \cdots d_{n-1})^2 \operatorname{disc}\left(1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{n-1}(\alpha)}{d_{n-1}}\right) = (d_1 \cdots d_{n-1})^2 \operatorname{disc}(R)$$

With respect to the basis $1, f_1(\alpha)/d_1, \dots, f_{n-1}(\alpha)/d_{n-1}$, R is generated freely by the vectors $e_0, \dots, e_{n-1}$ and $\mathbb{Z}[\alpha]$ is generated freely by $e_0, d_1 e_1, \dots, d_{n-1} e_{n-1}$. So, the quotient is the product of the cyclic groups $\mathbb{Z}/d_i\mathbb{Z}$ for $i = 1, \dots, n-1$. Thus, $R/\mathbb{Z}[\alpha]$ has order $d_1 \cdots d_{n-1}$.

For i, j with $i + j < n$, we have $f_i(\alpha)/d_i$ and $f_j(\alpha)/d_j$ are in R, so their product is as well, i.e. $f_i(\alpha) f_j(\alpha)/(d_i d_j) \in R$. But this is $d_i d_j$ over a monic polynomial in α of degree $i + j$, so the leading term comes from an integer multiple of $f_{i+j}(\alpha)/d_{i+j}$. I.e. there is some $n \in \mathbb{Z}$ with $n/d_{i+j} = 1/(d_i d_j)$, so that $d_{i+j} = n d_i d_j$. This shows $d_i d_j \mid d_{i+j}$ as claimed.

Finally, similarly, we have $(f_1(\alpha)/d_1)^i$ is in R, and it is a monic polynomial in α of degree i divided by d_1^i, so we have $n/d_i = 1/d_1^i$ for some $n \in \mathbb{Z}$. I.e. $n d_1^i = d_i$, so $d_1^i \mid d_i$ as claimed. Thus, $d_1^{2i} \mid d_i^2$ for each i, and taking the product $i = 1, \dots, n-1$ gives:

$$d_1^{2+4+\cdots+2(n-1)} \mid \prod_{i=1}^{n-1} d_i^2 \mid \operatorname{disc}(\alpha)$$

where the final divisibility comes from the first part and the fact that $\operatorname{disc}(R)$ is an integer. But the first term here is $d_1^{(n-1)n}$, so this gives the claim. □

Exercise (2.41).

Proof. The minimal polynomial for α over $\mathbb{Q}$ is $f(x) = x^3 - m$, so we can compute the discriminant (since α has degree 3) via:

$$\operatorname{disc}(\alpha) = -N(f'(\alpha)) = -N(3\alpha^2) = -27N(\alpha)^2 = -27m^2$$

where $N(\alpha) = m$ again comes from the minimal polynomial. Hence, from the previous problem, we get $d_1^6 = d_1^{n(n-1)} \mid \operatorname{disc}(\alpha) = -27m^2$. Since m is cubefree, m^2 is sixth-power-free, i.e. the only possible prime divisor of d_1 is 3, and $9 \nmid d_1$ since $3^{12} \nmid 3^3 m^2$. So, $d_1 = 1$ or $d_1 = 3$, and in the latter case $9 \mid m$.

Suppose that $d_1 = 3$, so that $9 \mid m$. Then the first basis element is $\beta = f_1(\alpha)/d_1 = (\alpha + b)/3$ for some $b \in \mathbb{Z}$. Then,

$$\beta^3 = \frac{1}{27}(m + 3\alpha^2 b + 3\alpha b^2 + b^3)$$

We have $T(\alpha) = 0$ from the minimal polynomial. We have $(\alpha^2)^3 - m^2 = 0$ and α^2 has degree 3 over $\mathbb{Q}$ since $\mathbb{Q} \subsetneq \mathbb{Q}(\alpha^2) \subseteq \mathbb{Q}(\alpha)$. So, $x^3 - m^2$ is the minimal polynomial of α^2, which gives $T(\alpha^2) = 0$ as well. Thus,

$$T(\beta^3) = \frac{1}{27}(3m + 3b^3) = \frac{m + b^3}{9}$$

Since $9 \mid m$ and $T(\beta^3) \in \mathbb{Z}$, we have $9 \mid b^3$, i.e. $3 \mid b$. So, $b/3 \in \mathbb{Z} \subseteq R$, so $\alpha/3 = \beta - b/3 \in R$, but $\alpha/3 \notin R$, since it has minimal polynomial $x^3 - m/27$, which doesn't have integer coefficients. So, the contradiction gives $d_1 = 1$. By exercise 39, we may assume $f_1(x) = x$.

Note that

$$(\alpha^2/k)^3 = \alpha^6/k^3 = m^2/k^3 = h^2 k^4/k^3 = h^2 k \in \mathbb{Z}$$

So, α^2/k satisfies $x^3 - h^2k$ and is an algebraic integer. Note that this gives $k \mid d_2$.

Consider $m \equiv \pm 1 \pmod 9$. Then, for $\beta = (\alpha \mp 1)^2/3$, we have

$$\begin{aligned}
&27\left(\beta^3 - \beta^2 + \frac{1 \pm 2m}{3}\beta - \frac{(m \mp 1)^2}{27}\right) \\
&= (3\beta)^3 - 3(3\beta)^2 + 3(1 \pm 2m)(3\beta) - (m \mp 1)^2 \\
&= (\alpha \mp 1)^6 - 3(\alpha \mp 1)^4 + 3(1 \pm 2m)(\alpha \mp 1)^2 - (m \mp 1)^2 \\
&= (\alpha^6 \mp 6\alpha^5 + 15\alpha^4 \mp 20\alpha^3 + 15\alpha^2 \mp 6\alpha + 1) - 3(\alpha^4 \mp 4\alpha^3 + 6\alpha^2 \mp 4\alpha + 1) \\
&\quad + (3 \pm 6m)(\alpha^2 \mp 2\alpha + 1) - (m^2 \mp 2m + 1) \\
&= (\mp 6m + 15 - 18 + 3 \pm 6m)\alpha^2 + (15m \mp 6 - 3m \pm 12 \mp 6 - 12m)\alpha \\
&\quad + (m^2 \mp 20m + 1 \pm 12m - 3 + 3 \pm 6m - m^2 \pm 2m - 1) \\
&= 0
\end{aligned}$$

So, β satisfies this polynomial. We have $1 \pm 2m \equiv 3 \pmod 9$, so the linear coefficient is an integer. We also have $m \mp 1 \equiv 0 \pmod 9$, so its square is a multiple of 81, hence the constant term is an integer (even a multiple of 3). So $\beta \in R$.

Since $m \equiv \pm 1 \pmod 9$, we have $3 \nmid k$. So, $k^2 \equiv 1 \pmod 3$, whence there is some $n \in \mathbb{Z}$ with $k^2 - 1 = 3n$. Then, since $\alpha, \alpha^2/k, \beta \in R$, so is $k\beta - n\alpha^2/k \pm k\alpha$. But this is:

$$k\beta - n\frac{\alpha^2}{k} \pm k\alpha = \frac{k(\alpha \mp 1)^2}{3} - \frac{n\alpha^2}{k} \pm k\alpha = \frac{k^2\alpha^2 \mp 2k^2\alpha + k^2 - 3n\alpha^2 \pm 3k^2\alpha}{3k} = \frac{\alpha^2 \pm k^2\alpha + k^2}{3k}$$

as claimed.

From the previous problem, we get that $d_2^2 \mid \operatorname{disc}(\alpha) = -27m^2$. So, for each prime, we have $2v_p(d_2) \le 3v_p(3) + 2v_p(m)$. For $p \neq 3$, this gives $v_p(d_2) \le v_p(m) = v_p(3m)$ as desired. For $p = 3$, we have $v_p(d_2) \le 3/2 + v_p(m)$, so $v_p(d_2) \le 1 + v_p(m) = v_p(3m)$ as well, since the equation is in integers, and so we get $d_2 \mid 3m$.

Since $p \mid d_2$ and $f_2(\alpha)/d_2 \in R$, we have $\gamma = (\alpha^2 + a\alpha + b)/p = f_2(\alpha)/d_2 \cdot (d_2/p) \in R$ as claimed. We already computed $T(\alpha) = T(\alpha^2) = 0$, so $T(\gamma) = 3b/p \in \mathbb{Z}$. So, $p \mid 3b$, and since $p \neq 3$ we have $p \mid b$. So b/p is an integer and so $\gamma - b/p \in R$ whence $(\gamma - b/p)^3 \in R$. We have

$$(\gamma - b/p)^3 = \frac{\alpha^6 + 3a\alpha^5 + 3a^2\alpha^4 + a^3\alpha^3}{p^3} = \frac{3am\alpha^2 + 2a^2m\alpha + (m^2 + ma^3)}{p^3}$$

So, taking traces gives $p^3 \mid 3m(m + a^3)$. Since $p \neq 3$ we get $p^3 \mid m(m + a^3)$ again. Since $p \mid m$ but $p^2 \nmid m$, this gives $p^2 \mid m + a^3$. But again, $p \mid m$, so this gives $p \mid a^3$, so $p \mid a$, so $p^3 \mid a^3$. But then p^2 divides both $m + a^3$ and a^3, so we get $p^2 \mid m$, contrary to assumption.

Now, suppose $p \neq 3$ and $p^2 \mid m$. Then $p^2 \mid hk^2$, so $p^2 \mid h$ or $p^2 \mid k^2$, but not both since they are coprime. But the first is impossible since h is squarefree, so $p \mid k \mid d_2$. We want to show $p^2 \nmid d_2$, so suppose $p^2 \mid d_2$ for contradiction. Mimicking the argument above, we have $f_2(\alpha)/p^2 \in R$, so by taking traces we get $p^2 \mid 3b$, whence $p^2 \mid b$ and so $(\alpha^2 + a\alpha)/p^2 \in R$. Cubing again gives:

$$\frac{m(\alpha^3 + 3a\alpha^2 + 3a^2\alpha + a^3)}{p^6} \in R$$

So, taking the trace gives $p^6 \mid m(m + a^3)$. So, $p^4 \mid m + a^3$, so $p \mid a^3$, so p^3 divides both $m + a^3$ and a^3, whence $p^3 \mid m$, contradicting that m is cubefree.

As suggested, we note that $(f_2(\alpha)/d_2)^2 \in R$, and we know $d_2 R \subseteq \mathbb{Z}[\alpha]$, so:

$$\frac{\alpha^4 + 2a\alpha^3 + (a^2 + 2b)\alpha^2 + 2ab\alpha + b^2}{d_2} = \frac{(a^2 + 2b)\alpha^2 + (2ab + m)\alpha + (b^2 + 2am)}{d_2} \in \mathbb{Z}[\alpha]$$

So, by uniqueness of representations, we get that d_2 divides each of $a^2 + 2b$, $2ab + m$, and $b^2 + 2am$, as desired.

Everything we've done has shown that for $p \neq 3$ prime, that $v_p(d_2) = v_p(k) = v_p(3k)$. Finally we do the casework to determine $v_3(d_2)$. First, suppose $m \equiv \pm 1 \pmod 9$. Then, we have $3 \mid d_2$ since we've shown that $(\alpha^2 \pm k^2\alpha + k^2)/(3k) \in R$ in this case, but we have $9 \nmid d_2$ since $d_2 \mid 3m$. We also have $v_3(k) = 0$ since $3 \nmid m$, so we get $v_3(d_2) = 1 = v_3(3k)$. Hence in this case $d_2 = 3k$ and we get the integral basis:

$$1, \alpha, \frac{\alpha^2 \pm k^2\alpha + k^2}{3k}$$

in this case.

In all other cases, I will show that $v_3(d_2) = v_3(k)$, so that $d_2 = k$. Then, we will conclude that

$$1, \alpha, \frac{\alpha^2}{k}$$

is an integral basis for R over $\mathbb{Z}$. Our second case is when $m \equiv 4, 7 \pmod 9$. Suppose $3 \mid d_2$. Then $3 \nmid b$, else 3 divides both b, and $2ab + m$, whence it divides m, contrary to assumption. Then, $b \equiv a^2 \equiv 1 \pmod 3$, and $1 \equiv m \equiv ab \equiv a \pmod 3$. So

$$\frac{(\alpha - 1)^2}{3} = \frac{\alpha^2 - 2\alpha + 1}{3} = \frac{\alpha^2 + a\alpha + b}{3} - \frac{(a+2)\alpha + (b-1)}{3} \in R$$

since the first term is our basis element and the second is in $\mathbb{Z}[\alpha]$ since $3 \mid a + 2, b - 1$. Then we also get $(\alpha - 1)^8/81 \in R$, and so taking the trace gives:

$$\frac{3(28\alpha^6 - 56\alpha^3 + 1)}{81} = \frac{28m^2 - 56m + 1}{27} \in \mathbb{Z}$$

So, $27 \mid m^2 - 2m + 1 = (m-1)^2$, so $9 \mid m - 1$, i.e. $m \equiv 1 \pmod 9$, contrary to assumption. So, we get $3 \nmid d_2$ and $k \mid d_2$ gives $3 \nmid k$, so that $v_3(d_2) = 0 = v_3(k)$ as claimed.

Third, suppose $m \equiv 2, 5 \pmod 9$, and again suppose $3 \mid d_2$. The same calculations above apply to get $b \equiv 1 \pmod 3$ but now give $2 \equiv m \equiv a \pmod 3$ this time. So,

$$\frac{(\alpha + 1)^2}{3} = \frac{\alpha^2 + 2\alpha + 1}{3} = \frac{\alpha^2 + a\alpha + b}{3} - \frac{(a-2)\alpha + (b-1)}{3} \in R$$

for the same reason as before. So, the fourth power is in R, and its trace is an integer, i.e.

$$\frac{28m^2 + 56m + 1}{27} \in \mathbb{Z}$$

whence $27 \mid m^2 + 2m + 1 = (m+1)^2$, so $9 \mid m + 1$, so $m \equiv -1 \pmod 9$, contrary to assumption. So again $v_3(d_2) = 0 = v_3(k)$.

Fourth, suppose $m \equiv \pm 3 \pmod 9$. Then again $3 \nmid k$, since otherwise $9 \mid k^2 \mid m$. Suppose $3 \mid d_2$. Then, we have $b^2 \equiv am \equiv 0 \pmod 3$, so $3 \mid b$, and $a^2 \equiv b \equiv 0 \pmod 3$, so $3 \mid a$ as well. So,

$$\frac{\alpha^2}{3} = \frac{\alpha^2 + a\alpha + b}{3} - \frac{a\alpha + b}{3} \in R$$

But this means $m^2/27 = (\alpha^2/3)^3 \in R \cap \mathbb{Q} = \mathbb{Z}$, so $27 \mid m^2$, so $9 \mid m$, contrary to assumption. So, $3 \nmid d_2$, and $v_3(d_2) = 0 = v_3(k)$ again.

Fifth and finally, suppose $m \equiv 0 \pmod 9$. Then $3 \mid k \mid d_2$ and $9 \nmid k$ since it's squarefree. It suffices to show $9 \nmid d_2$, since then $v_3(k) = 1 = v_3(d_2)$ and the proof will be complete. So, suppose $9 \mid d_2$. Then,

$$a^4 \equiv (-2b)^2 \equiv 4b^2 \equiv 4(-2am) \equiv 0 \pmod 9$$

so $3 \mid a$, so that $b \equiv 5a^2 \equiv 0 \pmod 9$. Then $f_2(\alpha) - b/9 = (\alpha^2 + a\alpha)/9 \in R$, and so its cube is also, so its trace is in $\mathbb{Z}$. I.e., $3^5 \mid m(m + a^3)$, so $3^3 \mid m + a^3$, but then $3 \mid a$ and $3^3 \mid a^3$, so that $3^3 \mid m$, contrary to m being cubefree. So, finally, we get $9 \nmid d_2$ as claimed, completing the proof. □

Exercise (2.42).

Proof. One direction is clear. Suppose $\alpha \in R$. Then $N^K_{\mathbb{Q}(\sqrt{m})}(\alpha)$ is the product of (some of the) conjugates of α, which are all algebraic integers, and so the product is also an algebraic integer. Similarly, $T^K_{\mathbb{Q}(\sqrt{m})}(\alpha)$ is the sum of algebraic integers, and so is also an algebraic integer.

Conversely, suppose that both this trace and norm are algebraic integers. Then consider the (monic) minimal polynomial of α over $\mathbb{Q}(\sqrt{m})$. Since $[K : \mathbb{Q}(\sqrt{m})] \leq 2$, this polynomial has two coefficients other than the leading coefficient, which are therefore this norm (the constant term) and trace (the linear term). I.e. α satisfies a monic polynomial with algebraic integer coefficients, so that α is itself an algebraic integer (see, e.g., exercise 4). Note that this proof only relies on $\mathbb{Q}(\sqrt{m}) \subseteq K$ being a degree 2 subextension. So, we reach the same conclusion about $\sqrt{n}, \sqrt{k}$.

Consider the case $m \equiv 3 \pmod 4$ and $n, k \equiv 2 \pmod 4$. Let $\alpha \in R$, so $\alpha = A + B\sqrt{m} + C\sqrt{n} + D\sqrt{k}$ for some $A, B, C, D \in \mathbb{Q}$ (since $\sqrt{k}$ is a $\mathbb{Q}$-multiple of $\sqrt{mn}$). Then, all of the traces are algebraic integers, so $2A+2C\sqrt{n}$, $2A+2B\sqrt{m}$, and $2A + 2D\sqrt{k}$ are all algebraic integers. Since m, n, k are squarefree and not congruent to 1 modulo 4, we get that each of the coefficients are integers, i.e. $A, B, C, D \in \frac{1}{2}\mathbb{Z}$, which gives the first result:

$$\alpha = \frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2}$$

for $a, b, c, d \in \mathbb{Z}$. Then, taking the trace over $\mathbb{Q}(\sqrt{m})$ gives that

$$\begin{aligned}
&\frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2} \cdot \frac{a + b\sqrt{m} - c\sqrt{n} - d\sqrt{k}}{2} \\
&\qquad = \frac{(a + b\sqrt{m})^2 - (c\sqrt{n} + d\sqrt{k})^2}{4} \\
&\qquad = \frac{a^2 + 2ab\sqrt{m} + mb^2 - nc^2 - 2cd\sqrt{nk} - kd^2}{4} \\
&\qquad = \frac{(a^2 + mb^2 - nc^2 - kd^2) + (2ab - 2cdn/\gcd(n, m))\sqrt{m}}{4}
\end{aligned}$$

is an algebraic integer. I.e. $4 \mid a^2 + mb^2 - nc^2 - kd^2$ and $4 \mid 2ab - 2cdn/\gcd(n, m)$. Since m is odd, $\gcd(n, m)$ is odd, so $2cdn/\gcd(m, n)$ is a multiple of 4. So, $4 \mid 2ab$, so $2 \mid ab$, and at least one is even. We have:

$$2(c^2 + d^2) \equiv nc^2 + kd^2 \equiv a^2 + mb^2 \equiv a^2 - b^2 \pmod 4$$

But then $a^2 - b^2$ is even, so $a \equiv b \pmod 2$. Since one is even, both are. Thus the above equation is zero throughout (mod 4), so $c^2 + d^2$ is even, which means $c \equiv d \pmod 2$ as well. Conversely, if a, b are even and c, d have the same parity, then it is clear that $N^K_{\mathbb{Q}(\sqrt{m})}(\alpha)$ is an algebraic integer. Thus, α is a $\mathbb{Z}$-linear combination of

$$1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n} + \sqrt{k}}{2}$$

and each of these is an algebraic integer. So, it's an integral basis.

CASES C,D OMITTED FOR NOW.

Note that $\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m}, \sqrt{k})$ since $\sqrt{n} = \gcd(m, n)\sqrt{k}/\sqrt{m}$. So, we can interchange n, m, k in any order. Thus we've covered all cases. Indeed, we summarize the cases for $m, n, k \pmod 4$ in the below table, using the fact that $k = nm/\gcd(m, n)^2$, along with which case (b/c/d) covers it:

m	n	k	Case
1	1	1	(d)
1	2	2	(c)
1	3	3	(c)
2	2	± 1	(b),(c)
2	3	2	(b)
3	3	1	(c)

In particular, if m, n are not both even, then $\gcd(m, n)$ is odd, so $\gcd(m, n)^2 \equiv 1 \pmod 4$ and $k \equiv mn \pmod 4$.

In all cases, we have

$$\begin{aligned}\operatorname{disc}_{\mathbb{Q}}^{K}(1,\sqrt{m},\sqrt{n},\sqrt{mn}) &= \operatorname{disc}_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{m})}(1,\sqrt{m})^2 N_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{m})}(\operatorname{disc}_{\mathbb{Q}(\sqrt{m})}^{K}(1,\sqrt{n})) \\ &= (4m)^2 N_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{m})}(4n) \\ &= (16mn)^2\end{aligned}$$

Multiplying the last term by $1/\gcd(m,n)$ gives:

$$\operatorname{disc}(1,\sqrt{m},\sqrt{n},\sqrt{k}) = \frac{(16mn)^2}{\gcd(m,n)^2} = 256mnk$$

We adjust this for each of the following cases.

In case (b), we can write the basis in terms of our given elements using the matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1/2 \\ 0 & 0 & 0 & 1/2 \end{pmatrix}$$

Thus, the discriminant of the ring in case (b) is $256mnk/2^2 = 64mnk$ as claimed. In this case, the three quadratic subfields have discriminants $4m, 4n, 4k$, respectively, so we get $64mnk = (4m)(4n)(4k)$, also as claimed.

In case (c), we have the change of basis matrix:

$$\begin{pmatrix} 1 & 1/2 & 0 & 0 \\ 0 & 1/2 & 0 & 0 \\ 0 & 0 & 1 & 1/2 \\ 0 & 0 & 0 & 1/2 \end{pmatrix}$$

Thus, the discriminant of the ring in case (c) is $256mnk/4^2 = 16mnk = (m)(4n)(4k)$.

In case (d), we swap n, k in the basis and have the change of basis matrix:

$$\begin{pmatrix} 1 & 1/2 & 1/2 & 1/4 \\ 0 & 1/2 & 0 & 1/4 \\ 0 & 0 & 0 & 1/4 \\ 0 & 0 & 1/2 & \gcd(m,n)/4 \end{pmatrix}$$

Thus, the discriminant of the ring in this case is $256mnk/(-16)^2 = mnk$, which is exactly the product of m, n, k, the discriminants of the quadratic subfields. □

Exercise (2.43).

Proof. We have:

$$\operatorname{disc}(\alpha) = N(f'(\alpha)) = N(5\alpha^4 + a) = \frac{N(5\alpha^5 + a\alpha)}{N(\alpha)} = \frac{N(5(-a\alpha - b) + a\alpha)}{-b} = \frac{N(4a\alpha + 5b)}{b}$$

To find this last norm, we need to multiply the conjugates. We have:

$$f(x) = \prod_i (x - \alpha_i)$$

where the α_i denote the five conjugates of α. So,

$$\begin{aligned}N(4a\alpha + 5b) &= \prod_i (4a\alpha_i + 5b) \\ &= (-4a)^5 \prod_i \left(-\frac{5b}{4a} - \alpha_i\right) \\ &= -4^5 a^5 f\left(-\frac{5b}{4a}\right) \\ &= -4^5 a^5 \left(-\frac{5^5 b^5}{4^5 a^5} - a\frac{5b}{4a} + b\right) \\ &= 5^5 b^5 + (4^4 5 - 4^5) a^5 b\end{aligned}$$

So, overall, we get:

$$\operatorname{disc}(\alpha) = \frac{5^5 b^5 + 4^4 a^5 b}{b} = 5^5 b^4 + 4^4 a^5$$

as claimed.

When $a = b = -1$, $\operatorname{disc}(\alpha) = 5^5 - 4^4 = 3125 - 256 = 2869 = 19 \cdot 151$, is squarefree. So, the ring of integers is $\mathbb{Z}[\alpha]$.

In this case, we have

$$\operatorname{disc}(\alpha) = a^4(4^4 a + 5^5)$$

The latter factor is squarefree, and a is squarefree, so $\operatorname{disc}(R)$ must be one of $\operatorname{disc}(\alpha), \operatorname{disc}(\alpha)/a^2, \operatorname{disc}(\alpha)/a^4$. I.e. we have $d_1 \mid d_2 \mid d_3 \mid d_4$ and $(d_1 d_2 d_3 d_4)^2$ is one of $1, a^2, a^4$, i.e. $d_1 d_2 d_3 d_4$ is one of $1, a, a^2$. This forces $d_1 = 1$, since $d_1^4 \mid d_1 d_2 d_3 d_4 \mid a^2$ and a is squarefree. Similarly, $d_2 = 1$ since $d_2^3 \mid d_1 d_2 d_3 d_4 \mid a^2$. So, we're left with $d_3 d_4 = d_1 d_2 d_3 d_4 \mid a^2$ as claimed.

For the explicit computations, first note the hint is true, for if m is not squarefree, then it is divisible by p^2 for some prime p. Then either $m = p^2$ is a square, or else m/p^2 has a prime factor q. If r is the smallest prime divisor of m, then $m \geq p^2 q \geq r^3$, so $r \leq \sqrt[3]{m}$.

Let $\gamma = 4^4 a + 5^5$. We're considering $-20 < a < 0$, so $\gamma < 5^5 = 3125$ and

$$\gamma > 5^5 \left(-20\frac{4^4}{5^5} + 1\right) = 5^5 \left(-20\frac{2^{13}}{10^5} + 1\right) = 5^5 \left(-20\frac{8192}{100000} + 1\right) > 5^5 \left(-20\frac{10000}{100000} + 1\right) = -5^5$$

So, we only need to consider primes p with $p^3 < 5^5$. Since $5^5 = 3195 < 4096 = 2^{12} = 16^3$, we only need to consider $p = 2, 3, 5, 7, 11, 13$. Clearly $4^4 a + 5^5$ isn't a multiple of either 2 or 5^2, so we only consider $p = 3, 7, 11, 13$.

We'll compute the cases directly. When $a = -2$:

$$4^4 a + 5^5 = 3125 - 512 = 2613 = 3 \cdot 13 \cdot 67$$

which is clearly squarefree.

When $a = -3$,

$$4^4 a + 5^5 = 3125 - 768 = 2357$$

This isn't divisible by either 3 or 11 (considering the sum and alternating sum of the digits). If $7 \mid 2357$, then $7 \mid 2350 = 10 \cdot 5 \cdot 47$, but clearly it doesn't divide any of these factors. Similarly, if $13 \mid 2357$ then $13 \mid 2370 = 10 \cdot 237$, so $13 \mid 237$. But then $13 \mid 250 = 2 \cdot 5^3$, which it doesn't. We're done if γ is not a square, but $\gamma \equiv 2 \pmod 3$, so it cannot be a square. So, in this case γ is squarefree.

When $a = -6$,

$$4^4 a + 5^5 = 3125 - 6 \cdot 256 = 1589 = 7 \cdot 227$$

and 227 is prime so γ is squarefree.

When $a = -7$,

$$\begin{aligned}
4^4 a + 5^5 &\equiv a + 2 \equiv 1 && \pmod 3 \\
4^4 a + 5^5 &\equiv (-2)^5 \equiv -32 \equiv 3 && \pmod 7 \\
4^4 a + 5^5 &\equiv 16^2 \cdot 4 + 25^2 \cdot 5 \equiv 5^2 \cdot 4 + 3^2 \cdot 5 \equiv 3 \cdot 4 + 9 \cdot 5 \equiv 1 + 1 \equiv 2 && \pmod{11} \\
4^4 a + 5^5 &\equiv 16^2 \cdot 6 + 25^2 \cdot 5 \equiv 9 \cdot 6 + 5 \equiv 7 && \pmod{13}
\end{aligned}$$

So it isn't divisible by any of these primes and isn't a square since 3 is a quadratic nonresidue mod 7.

When $a = -10$,

$$4^4 a + 5^5 = 3125 - 2560 = 565 = 5 \cdot 113$$

which is again clearly squarefree.

When $a = -11$,

$$4^4 a + 5^5 = 565 - 256 = 309 = 3 \cdot 103$$

which is squarefree.

When $a = -13$,

$$4^4 a + 5^5 = 309 - 512 = -203 = -7 \cdot 29$$

which is squarefree.

When $a = -15$,

$$4^4 a + 5^5 = -203 - 512 = -715 = -5 \cdot 143 = -5 \cdot 11 \cdot 13$$

which is squarefree.

Ignoring the hint, we have:

$$N(1+\alpha) = \prod_i (1+\alpha_i) = (-1)^5 \prod_i (-1-\alpha_i) = -f(-1) = -((-1)^5 + a(-1) + a) = 1$$

so $1+\alpha$ is a unit. □

Exercise (2.44).

Proof. As above, we have:

$$\operatorname{disc}(\alpha) = N(f'(\alpha)) = N(5\alpha^4 + 4a\alpha^3) = N(\alpha)^3 N(5\alpha + 4a) = (-b)^3 N(5\alpha + 4a)$$

and we compute the second term by considering the conjugates:

$$\begin{aligned} N(5\alpha + 4a) &= \prod_i (5\alpha_i + 4a) \\ &= (-5)^5 \prod_i (-4a/5 - \alpha_i) \\ &= -5^5 f(-4a/5) \\ &= -5^5 \left(-\frac{4^5 a^5}{5^5} + a\frac{4^4 a^4}{5^4} + b \right) \\ &= 4^5 a^5 - 4^4 5 a^5 - 5^5 b \\ &= 4^4(4-5)a^5 - 5^5 b \\ &= -(4^4 a^5 + 5^5 b) \end{aligned}$$

So, overall,

$$\operatorname{disc}(\alpha) = b^3(4^4 a^5 + 5^5 b)$$

As before, we have

$$b^3(4^4 a^5 + 5^5 b) = (d_1 d_2 d_3 d_4)^2 \operatorname{disc}(R)$$

where $d_1 \mid d_2 \mid d_3 \mid d_4$. Suppose p is a prime divisor of d_3. Then $p \mid d_4$, so $p^4 \mid (d_3 d_4)^2 \mid b^3(4^4 a^5 + 5^5 b)$. Since b and $4^4 a^5 + 5^5 b$ are squarefree, this is only possible if each is divisible by p (and not p^2, of course). But then $p \mid 4^4 a^5 \mid (2a)^8$, so $p \mid 2a$, which contradicts $\gcd(b, 2a) = 1$. So, such a prime cannot exist, i.e. $d_3 = 1$, and since $d_1 \mid d_2 \mid d_3$, they are all equal to 1.

Finally, we have $d_4^2 \mid b^3(4^4 a^5 + 5^5 b)$. If $p \mid d_4$, then p^2 divides this expression, and so p divides both b and $4^4 a^5 + 5^5 b$. Further, $p^2 \nmid d_4$ in this case, else we would again be in the above case where $b^3(4^4 a + 5^5 b)$ is divisible by p^4. So, $v_p(d_4) = 1 = v_p(b)$, whence $d_4 \mid b$.

When $a = -2$ and $b = 5$, we get

$$\operatorname{disc}(\alpha) = 5^3(4^4(-2)^5 + 5^5(5)) = 5^3(15625 - 8192) = 5^3 \cdot 7433$$

and 7433 is squarefree since it isn't divisible by any of 2, 3, 5, 7, 11, 13, 17, or 19, while $7433 < 8000 = 20^3$, and $7433 \equiv 2 \pmod 3$ so it isn't a perfect square.

For the case $a = b$, $\operatorname{disc}(\alpha) = a^4((4a)^4 + 5^5) = (d_1 d_2 d_3 d_4)^2 \operatorname{disc}(R)$. If a and $(4a)^4 + 5^5$ are squarefree, then $d_2^6 \mid a^4((4a)^4 + 5^5)$, implies that $d_2 = 1$, which gives $d_1 = 1$. So, we have $(d_3 d_4)^2 \mid a^4((4a)^4 + 5^5)$. For each prime divisor p of $d_3 d_4$, we have $2v_p(d_3 d_4) \le 4v_p(a) + v_p((4a)^4 + 5^5) \le 4v_p(a) + 1$. Since these are integers, this gives $2v_p(d_3 d_4) \le 4v_p(a)$, i.e. $v_p(d_3 d_4) \le v_p(a^2)$, and since this is true for all primes, we get $d_3 d_4 \mid a^2$.

Similarly, when $a = -b$, $\operatorname{disc}(\alpha) = a^4((4a)^4 - 5^5) = (d_1 d_2 d_3 d_4)^2 \operatorname{disc}(R)$. So, if a and $(4a)^4 - 5^5$ are squarefree, then $d_2^6 \mid a^4((4a)^4 - 5^5)$, so $d_2 = 1 \implies d_1 = 1$. Then $d_3 d_4 \mid a^2$ as in the previous case.

Finally, in the case $a = b$, we have $a(\alpha^4 + 1) = -\alpha^5$. Taking norms gives:

$$N(\alpha^4 + 1) = \frac{N(-\alpha^5)}{N(a)} = \frac{(-1)^5 N(\alpha)^5}{a^5} = \frac{-(-a)^5}{a^5} = 1$$

so $\alpha^4 + 1$ is a unit. In the case $a = -b$, we have $a(\alpha^4 - 1) = -\alpha^5$, so

$$N(\alpha^4 - 1) = \frac{N(-\alpha^5)}{N(a)} = \frac{(-1)^5(-a)^5}{a^5} = 1$$

so $\alpha^4 - 1$ is a unit. □

Exercise (2.45).

Proof. We repeat the process in the past few problems. If α is a root of an irreducible polynomial $f(x) = x^n + ax + b$ for $a, b \in \mathbb{Z}$, then

$$\begin{aligned}
\operatorname{disc}(\alpha) &= (-1)^{(n^2-n)/2} N(f'(\alpha)) \\
&= (-1)^{(n^2-n)/2} N(n\alpha^{n-1} + a) \\
&= (-1)^{(n^2-n)/2} \frac{N(n\alpha^n + a\alpha)}{N(\alpha)} \\
&= (-1)^{(n^2-n)/2} \frac{N(n(-a\alpha - b) + a\alpha)}{(-1)^n b} \\
&= (-1)^{(n^2+n)/2} \frac{N(a(1-n)\alpha - nb)}{b}
\end{aligned}$$

Then, letting $\alpha_1, \ldots, \alpha_n$ denote the conjugates of α, we have

$$f(x) = \prod_i (x - \alpha_i)$$

and so

$$\begin{aligned}
N(a(1-n)\alpha - nb) &= \prod_i (a(1-n)\alpha_i - nb) \\
&= [a(n-1)]^n \prod_i \left(\frac{nb}{a(1-n)} - \alpha_i \right) \\
&= [a(n-1)]^n f\left(\frac{nb}{a(1-n)} \right) \\
&= a^n (n-1)^n \left(\frac{n^n b^n}{a^n (1-n)^n} + a\frac{nb}{a(1-n)} + b \right) \\
&= (-nb)^n + (n-1)^{n-1} a^n b(n - 1 - n) \\
&= (-nb)^n - (n-1)^{n-1} a^n b
\end{aligned}$$

So, overall, we get:

$$\operatorname{disc}(\alpha) = (-1)^{(n^2+n)/2} \frac{(-nb)^n - (n-1)^{n-1} a^n b}{b} = (-1)^{(n^2-n)/2} \left(n^n b^{n-1} - (-1)^n (n-1)^{n-1} a^n \right)$$

Note that this agrees with our previous cases: when $n = 3$ (see exercise 28), we get

$$\operatorname{disc}(\alpha) = (-1)^3 (3^3 b^2 - (-1)^3 2^2 a^3) = -(27b^2 + 4a^3)$$

and when $n = 5$ (exercise 43):

$$\operatorname{disc}(\alpha) = (-1)^{10} (5^5 b^4 - (-1)^5 4^4 a^5) = 5^5 b^4 + 4^4 a^5$$

Similarly, suppose now that α is a root of the irreducible polynomial $f(x) = x^n + ax^{n-1} + b$ with $a, b \in \mathbb{Z}$. Then, writing the roots of f as $\alpha_1, \ldots, \alpha_n$, we get:

$$\begin{aligned}
\operatorname{disc}(\alpha) &= (-1)^{(n^2-n)/2} N(f'(\alpha)) \\
&= (-1)^{(n^2-n)/2} N(n\alpha^{n-1} + (n-1)a\alpha^{n-2}) \\
&= (-1)^{(n^2-n)/2} N(\alpha)^{n-2} N(n\alpha + (n-1)a) \\
&= (-1)^{(n^2-n)/2} ((-1)^n b)^{n-2} \prod_i (n\alpha_i + (n-1)a) \\
&= (-1)^{(n^2-n)/2} (-1)^{n^2-2n} b^{n-2} (-n)^n \prod_i \left(\frac{1-n}{n} a - \alpha_i \right) \\
&= (-1)^{(-n^2+n)/2} b^{n-2} n^n f\left(\frac{1-n}{n} a \right) \\
&= (-1)^{(-n^2+n)/2} b^{n-2} n^n \left(\frac{(1-n)^n}{n^n} a^n + a \frac{(1-n)^{n-1}}{n^{n-1}} a^{n-1} + b \right) \\
&= (-1)^{(-n^2+n)/2} b^{n-2} ((1-n)^{n-1} a^n (1-n+n) + bn^n) \\
&= (-1)^{(n^2-n)/2} b^{n-2} ((-1)^{n-1} (n-1)^{n-1} a^n + n^n b)
\end{aligned}$$

This agrees with the previous exercise when $n = 5$:

$$\operatorname{disc}(\alpha) = (-1)^{10} b^3 ((-1)^4 4^4 a^5 + 5^5 b) = b^3 (4^4 a^5 + 5^5 b)$$

□

Exercise (2.46).

Proof. Since $f'(r) = 0$, we have $f'(x) = (x - r)g(x)$ for some $g \in \mathbb{Q}[x]$. Since $r \in \mathbb{Z}$, f' and $x - r$ are in $\mathbb{Z}[x]$, so by Gauss' Lemma, $g \in \mathbb{Z}[x]$ as well. Then, if α_i are the roots of f, then:

$$\begin{aligned}
\operatorname{disc}(\alpha) &= \pm N(f'(\alpha)) \\
&= \pm N((\alpha - r)g(\alpha)) \\
&= \pm N(\alpha - r) N(g(\alpha)) \\
&= \pm N(g(\alpha)) \prod_i (\alpha_i - r) \\
&= \pm N(g(\alpha)) f(r)
\end{aligned}$$

Since g has integer coefficients, $g(\alpha)$ is an algebraic integer, so it has integral norm. So, this shows $f(r) \mid \operatorname{disc}(\alpha)$ as claimed.

More generally, suppose $f'(r/s) = 0$ for $\gcd(r, s) = 1$. Then we can write:

$$f'(x) = (x - r/s)g(x)$$

for some $g \in \mathbb{Q}[x]$. There is a rational number a/b such that ag/b is a primitive polynomial (integral polynomial with no common divisor of the coefficients). So, we get:

$$asf'(x)/b = (sx - r)ag(x)/b$$

Then $sx - r$ and ag/b are primitive, so by Gauss' Lemma, we get that asf'/b is primitive. But $f' \in \mathbb{Z}[x]$, so a divides all of the coefficients of asf'/b. Since it is primitive, this forces $a = 1$.

Similarly, $s/\gcd(s, b)$ divides all of the coefficients of sf'/b, which, by primitivity, gives $s/\gcd(s, b) = 1$, i.e. $s = \gcd(s, b)$, so $s \mid b$. I.e., $b = su$ for some $u \in \mathbb{Z}$.

So, $g/b \in \mathbb{Z}[x]$, and so does ug/b. That is, we are able to factorize

$$f'(x) = (x - r/s)g(x) = (sx - r)g(x)/s = (sx - r)ug(x)/(su) = (sx - r)ug(x)/b$$

as a product of $(sx - r)$ and an integer polynomial. Rename ug/b as g in the sequel, so we have $f'(x) = (sx - r)g(x)$.

Now, we proceed in the same way as before:

$$\begin{aligned}\operatorname{disc}(\alpha) &= \pm N(f'(\alpha)) \\ &= \pm N((s\alpha - r)g(\alpha)) \\ &= \pm N(g(\alpha)) \prod_i (s\alpha_i - r) \\ &= \pm N(g(\alpha)) s^n f(r/s)\end{aligned}$$

Since $s^n f(r/s)$ is an integer (the denominators clearly cancel), this gives $s^n f(r/s) \mid \operatorname{disc}(\alpha)$ in this case.

We have that $g(x)f'(x) = h(x) + f(x)k(x)$ for some polynomial $k \in \mathbb{Z}[x]$. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f; let $a_1, \ldots, a_r$ be the roots of g; let $b_1, \ldots, b_s$ be the roots of h; let G be the leading coefficient of g; and let H be the leading coefficient of h. By assumption, $a_j, b_j \in \mathbb{Q}$ for all j. Then,

$$\begin{aligned}\operatorname{disc}(\alpha) &= (-1)^{(n^2-n)/2} N(f'(\alpha)) \\ &= (-1)^{(n^2-n)/2} \frac{N(h(\alpha) + f(\alpha)k(\alpha))}{N(g(\alpha))} \\ &= (-1)^{(n^2-n)/2} \frac{N(h(\alpha))}{N(g(\alpha))} \\ &= (-1)^{(n^2-n)/2} \frac{\prod_i h(\alpha_i)}{\prod_i g(\alpha_i)} \\ &= (-1)^{(n^2-n)/2} \frac{\prod_i H \prod_{j=1}^s (\alpha_i - b_j)}{\prod_i G \prod_{j=1}^r (\alpha_i - a_j)} \\ &= (-1)^{(n^2-n)/2} \frac{H^n \prod_{j=1}^s \prod_i (\alpha_i - b_j)}{G^n \prod_{j=1}^r \prod_i (\alpha_i - a_j)} \\ &= (-1)^{(n^2-n)/2} \frac{H^n \prod_{j=1}^s (-1)^n f(b_j)}{G^n \prod_{j=1}^r (-1)^n f(a_j)} \\ &= (-1)^{(n^2-n)/2 + n(s+r)} \frac{H^n \prod_{j=1}^s f(b_j)}{G^n \prod_{j=1}^r f(a_j)}\end{aligned}$$

I.e., up to a constant, we only need the product of evaluating f at the roots of h over the roots of g to find the discriminant. □

Exercise (2.47).

Proof. Per the previous exercise, we should write f' as a rational function in $\mathbb{Z}[x]/f(x)$. We have

$$xf'(x) = x(5x^4 - 2x) = 5x^5 - 2x^2 \equiv 5(x^2 - 15) - 2x^2 = 3x^2 - 75 = 3(x-5)(x+5) \pmod{f(x)}$$

So, from the previous exercise,

$$\begin{aligned}\operatorname{disc}(\alpha) &= (-1)^{10+15} \frac{3^5 f(5) f(-5)}{1^5 f(0)} \\ &= -\frac{3^5(5^5 - 5^2 + 15)(-5^5 - 5^2 + 15)}{15} \\ &= -\frac{3^4}{5}(-10 + 5^5)(-10 - 5^5) \\ &= -\frac{3^4}{5}(100 - 5^{10}) \\ &= 3^4(5^9 - 20)\end{aligned}$$

□

Exercise (2.48).

Proof.

(a) Let $g(x) = f(x - a/3)$. I.e.,

$$\begin{aligned} g(x) &= (x - a/3)^3 + a(x - a/3)^2 + b(x - a/3) + c \\ &= x^3 + (3(-a/3) + a)x^2 + (3(-a/3)^2 - 2a(a/3) + b)x + f(-a/3) \\ &= x^3 - (d^2/3)x + f(-a/3) \end{aligned}$$

Now, let $\alpha_1, \alpha_2, \alpha_3$ denote the roots of f. Then g is also irreducible over $\mathbb{Q}$ with roots $\alpha_i + a/3$. Then,

$$\begin{aligned} \operatorname{disc}(\alpha) &= \prod_{1 \le r < s \le 3} (\alpha_r - \alpha_s)^2 \\ &= \prod_{1 \le r < s \le 3} [(\alpha_r + a/3) - (\alpha_s + a/3)]^2 \\ &= \operatorname{disc}(\alpha + a/3) \\ &= -N(g'(\alpha + a/3)) \end{aligned}$$

So, we compute g':

$$g'(x) = 3x^2 - d^2/3$$

I.e.

$$\begin{aligned} \operatorname{disc}(\alpha) &= -N(g'(\alpha + a/3)) \\ &= -N(3(\alpha + a/3)^2 - d^2/3) \\ &= -\prod_{i=1}^{3} \left(3\left(\alpha_i + \frac{a}{3}\right)^2 - \frac{d^2}{3} \right) \\ &= -27 \prod_{i=1}^{3} \left(\alpha_i + \frac{a}{3} - \frac{d}{3} \right) \left(\alpha_i + \frac{a}{3} + \frac{d}{3} \right) \\ &= -27 \prod_{i=1}^{3} \left(\frac{-a+d}{3} - \alpha_i \right) \left(\frac{-a-d}{3} - \alpha_i \right) \\ &= -27 f\left(\frac{-a+d}{3} \right) f\left(\frac{-a-d}{3} \right) \end{aligned}$$

as claimed.

(b) The same proof above still works for $d \notin \mathbb{Q}$. Namely, the only time we use d (as opposed to d^2) is in the final step, which is only a computation and does not rely on $d \in \mathbb{Q}$.

(c) We consider $xg'(x)$ modulo $g(x)$:

$$xg'(x) = 3x^3 - \frac{d^2}{3}x \equiv 3\left(\frac{d^2}{3}x - f(-a/3) \right) - \frac{d^2}{3}x = \frac{2d^2}{3}x - 3f\left(-\frac{a}{3}\right) \pmod{g(x)}$$

Note that the RHS has root $\frac{9f(-a/3)}{2d^2}$. So, by exercise (2.46):

$$\begin{aligned} \operatorname{disc}(\alpha) &= (-1)^9 \frac{\left(\frac{2d^2}{3}\right)^3 g\left(\frac{9f(-a/3)}{2d^2}\right)}{g(0)} \\ &= -\frac{8(a^2 - 3b)^3}{27 f(-a/3)} f\left(\frac{9}{2(a^2 - 3b)}(-a^3/27 + a^3/9 - ab/3 + c) - \frac{a}{3} \right) \\ &= \frac{8(3b - a^2)^3}{27 f(-a/3)} f\left(\frac{2a^3/3 - 3ab + 9c - a(2a^2 - 6b)/3}{2a^2 - 6b} \right) \\ &= \frac{8(3b - a^2)^3}{27 f(-a/3)} f\left(\frac{2a^3/3 - 3ab + 9c - 2a^3/3 + 2ab}{2a^2 - 6b} \right) \\ &= \frac{8(3b - a^2)^3}{27 f(-a/3)} f\left(\frac{9c - ab}{2a^2 - 6b} \right) \end{aligned}$$

as claimed.

(d) Finally, for the first explicit example, we have $a = -6$, $b = 9$, and $c = 3$. So,

$$f(-a/3) = f(2) = 8 - 6 \cdot 4 + 9 \cdot 2 + 3 = 5$$

and

$$a^2 - 3b = (-6)^2 - 3 \cdot 9 = 9$$

so

$$f\left(\frac{9c - ab}{2a^2 - 6b}\right) = f\left(\frac{9 \cdot 3 - (-6) \cdot 9}{2 \cdot 9}\right) = f(9/2) = 729/8 - 6(81/4) + 9(9/2) + 3 = \frac{105}{8}$$

giving

$$\operatorname{disc}(\alpha) = \frac{8(-9)^3(105/8)}{27(5)} = -3^4 7 = -567$$

Similarly, for the second, we have $a, b, c = -6, -9, 3$, respectively, so $a^2 - 3b = 36 + 27 = 63$ and:

$$\begin{aligned}
\operatorname{disc}(\alpha) &= \frac{8(-63)^3}{27 f(2)} f\left(\frac{27 - 54}{2(63)}\right) \\
&= -\frac{2^3 3^3 7^3}{8 - 24 - 18 + 3} f(-3/14) \\
&= -\frac{2^3 3^3 7^3}{-31}\left(-\frac{27}{14^3} - 6\frac{9}{14^2} + 9\frac{3}{14} + 3\right) \\
&= \frac{3^4}{31}(-9 - 18 \cdot 14 + 9 \cdot 14^2 + 14^3) \\
&= 3^4 137 = 11097
\end{aligned}$$

□