Exercise (0.1).

Proof. As noted, we need to characterize $a, b \in \mathbb{Q}$ such that $2a, a^2 - db^2 \in \mathbb{Z}$. Multiplying the second through by 4 gives $(2a)^2 - d(2b)^2 \in \mathbb{Z}$, whence $d(2b)^2 \in \mathbb{Z}$ since $2a \in \mathbb{Z}$, from which we get $2b \in \mathbb{Z}$ by prime factorization and the fact that d is squarefree. So, we may rewrite $a = x/2$ and $b = y/2$ for $x, y \in \mathbb{Z}$, and wish to characterize when $x^2 - dy^2$ is a multiple of 4. Finally, we consider cases: suppose $d \equiv 2, 3 \pmod 4$. If y is odd, then $x^2 - dy^2 \equiv x^2 - d \not\equiv 0 \pmod 4$ since d is not a square modulo 4. So instead, y must be even, whence x is also even and $\alpha = a + b\sqrt{d} = (x/2) + (y/2)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. So in this case $\mathbb{Z}[\sqrt{d}]$ is precisely the ring of integers.

On the other hand, suppose now $d \equiv 1 \pmod 4$. Then $x^2 - dy^2 \equiv x^2 - y^2 \equiv 0 \pmod 4$ whenever x and y have the same parity. I.e. the ring of integers is $\left\{\frac{x+y\sqrt{d}}{2} : x, y \in \mathbb{Z}, x \equiv y \pmod 2\right\} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Indeed, one can check that in this case the minimal polynomial for $(1+\sqrt{d})/2$ is $T^2 - T - (d-1)/4$. □

Exercise (0.2).

Proof. First, we simply verify the product:

$$(2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (4, 2+2\sqrt{-5}, -4+2\sqrt{-5})(9, 3+3\sqrt{-5}, 3-3\sqrt{-5}, 6) = (2)(3) = (6)$$

Here we've claimed that $(4, 2+2\sqrt{-5}, -4+2\sqrt{-5}) = (2)$ and $(9, 3+3\sqrt{-5}, 3-3\sqrt{-5}, 6) = (3)$. Let's verify the first of these. One containment is obvious: each generator on the left is a multiple of 2, and so is contained in the ideal (2). For the reverse, we need to show that 2 is in the ideal on the left, which is shown by the following calculation:

$$(2+2\sqrt{-5}) - (-4+2\sqrt{-5}) - (4) = 2$$

Let's now verify the factorization of (3). Again, one direction is obvious since each generator on the left is a multiple of 3. For the reverse, note that $9 - 6 = 3$, so 3 is contained in the ideal on the left. So the factorization is indeed as claimed.

Finally, let's check that this is a factorization into primes in $\mathbb{Z}[\sqrt{-5}]$. For each, we show that the quotient is a domain by lifting to the polynomial ring $\mathbb{Z}[T]$:

$$\mathbb{Z}[\sqrt{-5}]/(2, 1+\sqrt{-5}) = \mathbb{Z}[T]/(T^2+5, 2, 1+T) = \mathbb{F}_2[T]/(T^2+5, T+1) = \mathbb{F}_2[T]/(T+1) = \mathbb{F}_2$$

which is a domain. Note we used the fact that in $\mathbb{F}_2[T]$: $(T^2+5, T+1) = (T+1)$ since $T^2+5 = (T+1)^2$ is a multiple of $T+1$. Similarly:

$$\mathbb{Z}[\sqrt{-5}]/(3, 1+\sqrt{-5}) = \mathbb{Z}[T]/(T^2+5, 3, 1+T) = \mathbb{F}_3[T]/(T^2+5, T+1) = \mathbb{F}_3[T]/(T+1) = \mathbb{F}_3$$

since $T^2+5 = (T+1)(T-1)$ over $\mathbb{F}_3$. Finally,

$$\mathbb{Z}[\sqrt{-5}]/(3, 1-\sqrt{-5}) = \mathbb{Z}[T]/(T^2+5, 3, 1-T) = \mathbb{F}_3[T]/(T^2+5, T-1) = \mathbb{F}_3[T]/(T-1) = \mathbb{F}_3$$

for the same reason. These are all domains, so each of these ideals is indeed prime as claimed. □

Exercise (1.1).

Proof. [Note: this exercise does not require A to be a domain, so long as we are okay with multiplicative sets containing 0 (in which case the localization is trivial)]

Suppose first that S is a saturated multiplicative subset, and let T denote its complement. Let $x \in T$. I claim its image $x/1 \in S^{-1}A$ is not a unit. Indeed, if it were, then there would be $a/s \in S^{-1}A$ such that $(x/1)(a/s) = 1/1$, i.e. $u(ax - s) = 0$ for some $u \in S$. But then $uax = us \in S$ and by saturation, $x \in S$, contrary to assumption. So, $x/1$ is not a unit in $S^{-1}A$, whence it is contained in a prime ideal of $S^{-1}A$. But this corresponds precisely to a prime ideal P of A containing x that is disjoint from S. I.e. we've found a prime ideal of A contained in T that contains x. Taking the union over all $x \in T$ gives the result that T is a union of primes, as claimed.

Conversely, suppose that $T = \bigcup_i P_i$ is a union of prime ideals. Let $ab \in S$ for some $a, b \in A$. For each i, we have $ab \notin P_i$, so $a \notin P_i$ and $b \notin P_i$. So a, b are both not contained in the union of the P_i, i.e. they are not contained in T. In other words, they are contained in S.

Let $\mathscr{S}$ denote the collection of all saturated multiplicative subsets of A containing S. This is a nonempty collection since $A \in \mathscr{S}$, so we can consider $S' = \bigcap \mathscr{S}$. I claim S' is a saturated multiplicative subset of A. Indeed, if $ab \in S'$, then $ab \in U$ for each $U \in \mathscr{S}$, whence $a, b \in U$ for each such U, so that $a, b \in S'$. Further, it is clear that $1 \in S'$ since $1 \in U$ for each $U \in \mathscr{S}$, and it is clear that S' is closed under multiplication. This immediately handles the existence and uniqueness questions posed.

Now, we'd like to show $S' = A \setminus \bigcup \mathfrak{p}$. Let $V = A \setminus \bigcup \mathfrak{p}$ for notation. Note that V is a multiplicative set, for if $a, b \in V$, then $a, b \notin \mathfrak{p}$ for each indexed prime, so that $ab \notin \mathfrak{p}$ by primality, and $ab \in V$. Further, it is obvious that the complement of V is a union of primes, so V is saturated. By our definition of S', this gives $S' \subseteq V$. For the reverse, let $x \in V$. If $x/1$ is not a unit in $S^{-1}A$, then there is some prime ideal of $S^{-1}A$ containing $x/1$, which corresponds to a prime ideal of A disjoint from S containing x. But this precisely contradicts the definition of V. So, $x/1$ is a unit in $S^{-1}A$, which means it has an inverse a/s for some $a \in A$ and $s \in S$. That is, $ax/s = 1/1$, whence $uax = us$ for some $u \in S$, giving $uax \in S$. But then $uax \in S'$ since S' contains S, and since S' is saturated, $u, a, x \in S$. In particular, we've shown that $V \subseteq S'$, and so $V = S'$.

Consider now the localization maps $f : A \to S^{-1}A$ and $g : A \to S'^{-1}A$. First, note that if $s \in S$, then $s \in S'$, so $g(s) = s/1$ is a unit. By the universal property, we get a unique map $h : S^{-1}A \to S'^{-1}A$ with $g = h \circ f$. Similarly, the argument above shows that if $s \in S'$, then $f(s')$ is a unit in $S^{-1}A$ so we get a map $h' : S'^{-1}A \to S^{-1}A$ with $f = h' \circ g$. But then $g = (h \circ h') \circ g$ and $f = (h' \circ h) \circ f$, so by the uniqueness part of universal property, we get $h \circ h' = \mathrm{id}$ and $h' \circ h = \mathrm{id}$. I.e. $S^{-1}A \cong S'^{-1}A$. Note that in the case that A is a domain, this isomorphism is in fact equality when both localizations are considered as subrings of the field of fractions.

In summary, $S^{-1}A = S'^{-1}A$ and $S' = V$ is determined by the primes disjoint from S, which are precisely the primes in A that remain prime in $S^{-1}A$, explaining the claimed characterization. □

Exercise (2.1).

Proof. Note that $(\sqrt{5}+1)(\sqrt{5}-1) = 4 = 2 \cdot 2$. I claim these elements ($\sqrt{5} \pm 1$ and 2) are irreducible in $\mathbb{Z}[\sqrt{5}]$, demonstrating the failure of unique factorization. Indeed, suppose α is one of these three elements, and that it can be written as a product $\alpha = \beta\gamma$. Taking norms gives $N(\beta)N(\gamma) = N(\alpha) = \pm 4$. If $N(\beta) = \pm 1$, then it is a unit, and if $N(\beta) = \pm 4$, then γ is a unit and we're done. So, the only possibility remaining is that $N(\beta) = \pm 2$. Writing $\beta = u + v\sqrt{5}$ for integers u, v gives $u^2 - 5v^2 = \pm 2$. But modulo 4, this gives $(u-v)(u+v) \equiv 2 \pmod 4$, which is impossible since $u - v$ and $u + v$ have the same parity. □

Exercise (2.2).

Proof. Since f is reducible in $K[X]$, we can write $f = gh$ with $g, h \in K[X]$. Further, we may assume g, h are also monic by rescaling if necessary.

Now, let L be a splitting field for f over K, and let B be the integral closure of A in L. In $L[X]$, the polynomials g, h split completely since they are factors of f, which splits completely. Each root of g in L is a root of f, which is a monic polynomial with coefficients in A. So, each root of g is contained in B. The coefficients of g are polynomials in the roots with integer coefficients (here we use that g is monic), so the coefficients of g are then also in B, and so integral over A. But the coefficients of g are also elements of K by assumption, so since A is integrally closed in K, they must be in A itself. That is, $g \in A[X]$, and the same argument shows $h \in A[X]$, completing the proof. □

Exercise (2.3).

Proof. Note that if M/L and L/K are field extensions, then

$$\mathrm{disc}(M/K) = \mathrm{disc}(L/K)^{[M:L]} N_{L/K}(\mathrm{disc}(M/L))$$

So, to show that L/K inseparable has discriminant zero, it suffices to show this for some intermediate subextension. First, we can replace K with its separable closure in L and assume that L/K is purely inseparable. Now, it is known that any element of L has minimal polynomial $T^{p^r} - a$ for some $r \in \mathbb{Z}$ and $a \in K$. Choose an element $\alpha \in L \setminus K$ with minimal polynomial $f(T) = T^{p^r} - a$ and replace L with the extension $K[\alpha]$. Then a basis for the extension is $1, \alpha, \ldots, \alpha^{p^r - 1}$. With respect to this basis, the discriminant is:

$$\pm N(f'(\alpha)) = \pm N(p^r \alpha^{p^r - 1}) = \pm N(0) = 0$$

as desired. □

Exercise (2.4).

Proof. First, it is clear that $\mathfrak{a} \neq (2)$ since $1 + \sqrt{-3} \in \mathfrak{a}$, but $1 + \sqrt{-3} \notin (2)$ since $\frac{1+\sqrt{-3}}{2} \notin \mathbb{Z}[\sqrt{-3}]$ since $\{1, \sqrt{-3}\}$ is a basis for $\mathbb{Q}(\sqrt{-3})$ over $\mathbb{Q}$. Directly, we have:

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

This shows that we do not have uniqueness of factorization of ideals into primes. Indeed, if we did, then writing $(2) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ and $\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_m$ gives the distinct factorizations

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_m = \mathfrak{q}_1^2 \cdots \mathfrak{q}_m^2$$

for $\mathfrak{a}^2 = 2\mathfrak{a}$; if these were not distinct then we would conclude $\mathfrak{a} = (2)$. ☐

Exercise (2.5).

Proof. Let $\alpha \in A[\beta] \cap A[\beta^{-1}]$. Then $\alpha = f(\beta) = g(\beta^{-1})$ for polynomials $f, g \in A[x]$ of degrees m, n, respectively. Let $r = m + n - 1$ and consider the A-submodule $M = A \oplus \beta A \oplus \cdots \oplus \beta^r A$ of B. Since $1 \in M$, it now suffices to show that M is also an $A[\alpha]$-module, because then it is automatically faithful and clearly finitely generated.

In particular, it suffices to show that $\alpha\beta^i \in M$ for $i \in \{0, \dots, r\}$. For $i < n$, we have $\alpha\beta^i = f(\beta)\beta^i \in M$ because the exponents on β are all in the range $[i, m+i] \subseteq [0, r]$. For $i \geq n$, we have $\alpha\beta^i = g(\beta^{-1})\beta^i \in M$ since the exponents are in the range $[i-n, i] \subseteq [0, r]$. ☐

Exercise (2.6).

Proof. Note that $(1+\sqrt{7})(1-\sqrt{7}) = -6$ and $(1+\sqrt{10})(1-\sqrt{10}) = -9$ are both divisible by 3. Hence $3 \mid \alpha_i\alpha_j$ for $i \neq j$ since each product contains at least one of the above products.

On the other hand, the $\alpha_1, \dots, \alpha_4$ is a full set of conjugates, so $T(\alpha_i^n) = \sum_{j=1}^4 \alpha_j^n$. But modulo 3, this is the same as $(\sum_{j=1}^4 \alpha_j)^n$, since each of the cross terms is zero mod 3 as we've just shown. Explicitly, this is:

$$T(\alpha_i^n) \equiv (\alpha_1 + \cdots + \alpha_4)^n = 4^n \equiv 1^n = 1 \pmod{3\mathscr{O}_K}$$

In other words, $T(\alpha_i^n) - 1 = 3r$ for some $r \in \mathscr{O}_K$. But then r is integral over $\mathbb{Z}$ and is rational since $T(\alpha_i^n) - 1 \in \mathbb{Z}$, so $r \in \mathbb{Z}$. In other words, $T(\alpha_i^n) \equiv 1 \pmod{3\mathbb{Z}}$. But if $\alpha_i^n = 3\beta$ for some $\beta \in \mathscr{O}_K$, then $T(\alpha_i^n) = T(3\beta) = 3T(\beta) \in 3\mathbb{Z}$, contrary to what we've shown. So no power of α_i is a multiple of 3.

Now, we have

$$3 \mid g(\alpha) \text{ in } \mathbb{Z}[\alpha] \iff g(\alpha) \in 3\mathbb{Z}[\alpha] \iff \overline{g(\alpha)} \in \mathbb{Z}[\alpha]/(3) = \mathbb{Z}[x]/(3, f(x)) = \mathbb{F}_3[x]/(\bar{f}(x)) \iff \bar{f} \mid \bar{g} \text{ in } \mathbb{F}_3[x]$$

as claimed.

The first part of the claim is simply restating the divisibility results above. Since $\mathbb{F}_3[x]$ is a UFD (in fact a PID), we conclude that $\bar{f}$ doesn't divide $\bar{f}_i^n$ for all n, so $\bar{f}$ has an irreducible factor that doesn't divide $\bar{f}_i$. But since $\bar{f}$ divides $\bar{f}_i \cdot \bar{f}_j$, this irreducible factor must appear in the factorization of $\bar{f}_j$ for each $j \neq i$ as claimed.

As noted, $\bar{f}$ has at least 4 distinct irreducible factors now. It is also the reduction of the minimal polynomial of α, so it has degree at most 4 since $[\mathbb{Q}(\sqrt{7}, \sqrt{10}) : \mathbb{Q}] = 4$. So, each factor must be linear. But $\mathbb{F}_3[x]$ only has 3 distinct linear monic polynomials: $x, x-1, x-2$. This is our contradiction. ☐

Exercise (2.7).

Proof. First, it is clear that $S^{-1}B$ is integral over $S^{-1}A$. Indeed, for $b/s \in S^{-1}B$, since b is integral over A, we have

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$

for some $a_i \in A$. But then

$$(b/s)^n + a_{n-1}/s(b/s)^{n-1} + \cdots + a_0/s^n = (b^n + a_{n-1}b^{n-1} + \cdots + a_0)/s^n = 0$$

and for each i, it is clear that $a_i/s^{n-i} \in S^{-1}A$.

So, it remains to show that $S^{-1}B$ is integrally closed in L. Suppose that $\alpha \in L$ satisfies a monic polynomial with coefficients in $S^{-1}B$. I.e. for some $b_i \in B$ and $s_i \in S$:

$$\alpha^n + (b_{n-1}/s_{n-1})\alpha^{n-1} + \cdots + b_0/s_0 = 0$$

Let $s = s_0 \cdots s_{n-1}$ be the product. Then multiplying through by s^n cancels all of the denominators, so we get that $s\alpha$ satisfies a monic polynomial with coefficients in B, and so is integral over B. Since B is integrally closed in L, we conclude that $s\alpha \in B$. But then $s \in S$ as the product of elements of S, so $\alpha = (s\alpha)/s \in S^{-1}B$. ☐

Exercise (2.8).

Proof. Recall that localization is exact. We have the exact sequence of A-modules:

$$0 \to \mathfrak{p} \to A \to A/\mathfrak{p} \to 0$$

and we can localize it at $\mathfrak{p}$ to get:

$$0 \to \mathfrak{p}A_\mathfrak{p} \to A_\mathfrak{p} \to (A/\mathfrak{p})_\mathfrak{p} \to 0$$

On the other hand, we can recognize that $\mathfrak{p}$ corresponds to the ideal 0 in $A/\mathfrak{p}$, and so this final localization is the field of fractions. I.e. we have

$$0 \to \mathfrak{p}A_\mathfrak{p} \to A_\mathfrak{p} \to \mathrm{Frac}(A/\mathfrak{p}) \to 0$$

which is what we sought to show. □

Exercise (3.1).

Proof. No, $k[x, y]$ is not a Dedekind domain as (x) is a nonzero, non-maximal prime ideal. □

Exercise (3.2).

Proof. We've seen already that because $3, 7 \not\equiv 1 \pmod 4$ and are squarefree, the ring of integers of $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{7})$ are $\mathbb{Z}[\sqrt{3}]$ and $\mathbb{Z}[\sqrt{7}]$, respectively. To see that the ring of integers in $\mathbb{Q}(\sqrt{3}, \sqrt{7})$ is not $\mathbb{Z}[\sqrt{3}, \sqrt{7}]$, it suffices to show that $\alpha = \frac{\sqrt{3}+\sqrt{7}}{2}$ is integral over $\mathbb{Z}$, since clearly $\alpha \notin \mathbb{Z}[\sqrt{3}, \sqrt{7}]$.

But this is a direct manipulation. We have $(2\alpha)^2 = 3 + 7 + 2\sqrt{21}$, so

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

and so

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

completing the argument. □

Exercise (3.3).

Proof. First, suppose $p = x^2 + y^2$. Modulo 4, the only squares are 0 and 1, so we get that p must be one of $0, 1, 2$ mod 4. The first case is impossible since then p is divisible by 4, and the third case happens only for $p = 2$. Otherwise, we've shown $p \equiv 1 \pmod 4$ as claimed.

Conversely, suppose $p \equiv 1 \pmod 4$. Then $4 \mid p - 1 = |\mathbb{F}_p^\times|$, which is a cyclic group, so there is some $\alpha \in \mathbb{F}_p^\times$ of order 4. Thus, in $\mathbb{F}_p[x]$, the polynomial $x^2 + 1$ is reducible, namely as $(x - \alpha)(x + \alpha)$. Now, if we consider the ideal $(p) \subseteq \mathbb{Z}[i]$, we can compute:

$$\mathbb{Z}[i]/(p) = \mathbb{Z}[x]/(p, x^2 + 1) = \mathbb{F}_p[x]/(x^2 + 1)$$

which is not a domain as we've just shown that $x^2 + 1$ is reducible. So (p) is not prime and instead splits as a product of two prime ideals in $\mathbb{Z}[i]$. But this is a PID, so we get a factorization of p itself as a product $p = uv$ for $u, v \in \mathbb{Z}[i]$ primes. Taking norms gives $p^2 = N(u)N(v)$ and since neither of u, v is a unit, we conclude $N(u) = N(v) = p$. But if $u = x + iy$, then this gives $p = N(u) = x^2 + y^2$ as desired.

Suppose now that $p = x^2 + 2y^2$. The only squares mod 8 are $0, 1, 4$, so we conclude that $p \pmod 4$ is one of: $0, 1, 2, 3, 4, 6$. The cases $0, 4, 6$ are ruled out immediately since p would be even and not equal to 2. If $p \equiv 2 \pmod 8$, then $p = 2$. Otherwise, $p \equiv 1, 3 \pmod 8$ as claimed.

Conversely, suppose p is either 1 or 3 modulo 8. By quadratic reciprocity, -2 is a square mod p, so $x^2 + 2$ factors in $\mathbb{F}_p$. Similarly, we now consider the splitting of $(p) \subseteq \mathbb{Z}[\sqrt{-2}]$:

$$\mathbb{Z}[\sqrt{-2}]/(p) = \mathbb{Z}[x]/(x^2 + 2, p) = \mathbb{F}_p[x]/(x^2 + 2)$$

so (p) splits as a product of two primes. The rest of the argument is exactly as above, where we conclude by noting that $p = N(x + y\sqrt{-2}) = x^2 + 2y^2$.

Finally, suppose $p = x^2 + 3y^2$. Modulo 3, the squares are 0 and 1, so this gives that p is itself either 0 or 1 mod 3. If $p \equiv 0 \pmod 3$, then $p = 3$. Otherwise, $p \equiv 1 \pmod 3$ as claimed.

Conversely, suppose $p \equiv 1 \pmod 3$. Then $3 \mid p - 1 = |\mathbb{F}_p^\times|$, so as in the first case, there is some $\alpha \in \mathbb{F}_p$ of order 3. So, α satisfies $x^3 - 1$ but not $x - 1$, whence it satisfies their quotient: $(x^3 - 1)/(x - 1) = x^2 + x + 1$. We conclude that this polynomial is thus reducible in $\mathbb{F}_p[x]$. This gives the desired splitting of (p) in the ring of integers of $\mathbb{Q}(\sqrt{-3})$, which is $\mathbb{Z}(\zeta_3)$ for $\zeta_3 = (-1+\sqrt{-3})/2$ a primitive cube root of unity. Thus:

$$\mathbb{Z}[\zeta_3]/(p) = \mathbb{Z}[x]/(x^2+x+1, p) = \mathbb{F}_p[x]/(x^2+x+1)$$

Again, the argument continues as before, giving $p = N(a+b\zeta_3) = a^2-ab+b^2$. If a is even, we get $p = (a/2-b)^2+3(a/2)^2$ and if b is even we similarly get $p = (a-b/2)^2+3(b/2)^2$. Finally, if a, b are both odd, then we get $p = [(a+b)/2]^2+3[(a-b)/2]^2$. So, in any case, we are done. ☐

Exercise (3.4).

Proof. More directly, A is noetherian as the image of $k[T, U]$ under the map $T \mapsto X^2$ and $U \mapsto X^3$.

The above realizes A as the quotient $k[T, U]/(T^3-U^2)$. So, if $\mathfrak{p} \in A$ is a prime, it corresponds to a prime P of $k[T, U]$ containing T^3-U^2. But this is irreducible, so (T^3-U^2) is a height 1 prime and so either $P = (T^3-U^2)$, in which case $\mathfrak{p} = 0$ or else P has height 2, making it and $\mathfrak{p}$ both maximal. ☐

Exercise (4.1).

Proof. Let A be any domain and $B = A[x]$ the polynomial ring in one variable over A. Then B is a domain, A is a subring, and $\mathfrak{p} = (x)$ is a nonzero prime ideal, but $\mathfrak{p} \cap A = 0$. ☐

Exercise (4.2).

Proof. First, write the factorization of $\mathfrak{D}B$, and note that one of the factors is $\mathfrak{P}^{e(\mathfrak{D}/\mathfrak{P})}$. Then, similarly, write the factorization of $\mathfrak{P}A$ and note that one of the factors is $\mathfrak{p}^{e(\mathfrak{P}/\mathfrak{p})}$. Substitute the latter expression into the former to get the factorization of $\mathfrak{D}A$, which includes the factor

$$\left(\mathfrak{p}^{e(\mathfrak{P}/\mathfrak{p})}\right)^{e(\mathfrak{D}/\mathfrak{P})} = \mathfrak{p}^{e(\mathfrak{D}/\mathfrak{P})e(\mathfrak{P}/\mathfrak{p})}$$

By uniqueness of factorization, this exponent must be exactly $e(\mathfrak{D}/\mathfrak{p})$ as claimed.

The statement about inertial degrees is even more direct, since degrees multiply in towers of field extensions. Namely:

$$f(\mathfrak{D}/\mathfrak{P})f(\mathfrak{P}/\mathfrak{p}) = [C/\mathfrak{D} : B/\mathfrak{P}][B/\mathfrak{P} : A/\mathfrak{p}] = [C/\mathfrak{D} : A/\mathfrak{p}] = f(\mathfrak{D}/\mathfrak{p})$$

☐

Exercise (4.3).

Proof. Note that $\mathscr{O}_K = \mathbb{Z}[\alpha]$ since it has discriminant -31 which is prime. Hence we can find factorizations of primes by factoring $h(X) = X^3+X+1$ in $\mathbb{F}_p$. Let g denote the number of primes occuring in the factorization of $p\mathscr{O}_K$.

First, if p ramifies, then p must divide the discriminant. I.e. $p = 31$, and in this case,

$$h(X) = X^3+X+1 \equiv (X-3)(X-14)^2 \pmod{31}$$

So, the case $g = 2$, $e = (1, 2)$ and $f = (1, 1)$ (as it must by $\sum e_i f_i = 3$) occurs, and the other ramified case does not occur, namely $(e, f, g) = (3, 1, 1)$.

Now, we may assume that $e(\mathfrak{p}/p) = 1$ for each $\mathfrak{p}$ lying over p and that $p \neq 31$. If $g = 1$, then p is inert, which happens iff $h(X)$ is irreducible mod p iff h has no root mod p. This does happen, say for $p = 2$, since neither 0 nor 1 is a root in $\mathbb{F}_2$.

If $g = 2$, then we must have $f = (1, 2)$, so h factors as a linear polynomial and an irreducible quadratic. For $p = 3$, we get

$$h(X) = X^3+X+1 \equiv (X-1)(X^2+X+2) \pmod{3}$$

and the latter factor is irreducible is it does not have $0, 1, 2$ as a root in $\mathbb{F}_3$.

Finally, if $g = 3$, then h totally splits into (distinct) linear factors mod p. I haven't yet found such a p, but I can prove that one exists. First, let L be a splitting field for h over K, and note that L is Galois over $\mathbb{Q}$. Now $L = \mathbb{Q}[\beta]$ for some integral β with minimal polynomial $u \in \mathbb{Z}[X]$. I claim that for infinitely primes p, there exists an $n \in \mathbb{Z}$ such that $p \mid u(n)$ [Proven below]. In particular, there is one such prime that does not divide $|\mathscr{O}_L/\mathbb{Z}[\beta]|$ and is also not equal to 31. For this prime, the factorization of u gives the factorization of $p\mathscr{O}_L$. But since L is Galois and u has a root (n), u must split completely into linear factors, and so $p\mathscr{O}_L$ is the product of distinct primes of inertial degree 1. This completes the argument, since the inertial degree is multiplicative, and so $p\mathscr{O}_K$ is also the product of distinct primes of inertial degree 1.

To complete the proof, we prove the subclaim. Let $u \in \mathbb{Z}[x]$ be a nonconstant polynomial. Then I claim there are infinitely many primes p such that there exists an $n \in \mathbb{Z}$ with $p \mid u(n)$. First, suppose $u(0) = 1$. Then if P is any finite set of primes, consider $n = k\prod_{p\in P} p$ for any $k \in \mathbb{Z}$. We have $n \equiv 0 \pmod{p}$ for each $p \in P$ and so $u(n) \equiv u(0) = 1 \pmod{p}$. Since u is nonconstant, it takes the value 1 only finitely many times, and so for k sufficiently large, $u(n) \neq 1$ but is not divisible by any prime in P. So it must be divisible by some other prime, and this shows that no finite set of primes suffices. If $u(0) \neq 1$, then consider the polynomial $g(x) = u(u(0)x)/u(0)$. This still has integer coefficients by construction, and has $g(0) = u(0)/u(0) = 1$, so by the above, there are infinitely many primes p for which there exists an n such that $u(u(0)n)/u(0)$ is divisible by p. But then $u(u(0)n)$ itself is divisible by p, and so the claim is shown. □

Exercise (4.4).

Proof. Note that for $K = \mathbb{Q}(\sqrt{-23})$, the ring of integers is $\mathscr{O}_K = \mathbb{Z}[\alpha]$ for $\alpha = (1+\sqrt{-23})/2$ with minimal polynomial $f(x) = x^2 - x + 6$ and discriminant $\Delta = -23$. The Minkowski bound is:

$$\frac{2!}{2^2}\left(\frac{4}{\pi}\right)^1 |-23|^{1/2} = (2/\pi)\sqrt{23} < 4$$

So, each ideal class has an integral representative of norm 1, 2, or 3. The only integral ideal of norm 1 is $\mathscr{O}_K$ itself, representing the trivial ideal class. Any ideal of norm 2 divides (2), so we start by considering the factorization of 2, which requires factoring f mod 2:

$$f(x) = x^2 - x + 6 \equiv x(x-1) \pmod{2}$$

So $(2) = (2,\alpha)(2,\alpha-1)$ and each of these has norm 2. Similarly analyzing mod 3 gives:

$$f(x) = x^2 - x + 6 \equiv x(x-1) \pmod{3}$$

so that $(3) = (3,\alpha)(3,\alpha-1)$. Since $N(\alpha) = N(\alpha-1) = 6$, we get $(\alpha) = (2,\alpha)(3,\alpha)$ and $(\alpha-1) = (2,\alpha-1)(3,\alpha-1)$. So we get

$$(2,\alpha) \sim (3,\alpha)^{-1} \sim (3,\alpha-1) \sim (2,\alpha-1)^{-1}$$

where $\sim$ denotes equivalence of ideal classes. It remains to show that $(1), (2,\alpha), (2,\alpha-1)$ are pairwise distinct. To see that neither $(2,\alpha)$ nor $(2,\alpha-1)$ are principal, it suffices to show that no element of $\mathscr{O}_K$ has norm two. But

$$N(a+b\alpha) = (a+b\alpha)(a+b(1-\alpha)) = a^2 + ab + 6b^2 = \frac{1}{4}(2a+b)^2 + \frac{23}{4}b^2$$

If $b \neq 0$, then $N(a+b\alpha) \geq 23/4 > 2$, so it cannot be 2. So $b = 0$, and $N(a) = a^2 \neq 2$.

Finally, it remains to show that $(2,\alpha) \not\sim (2,\alpha-1)$, for which it suffices to show that $(2,\alpha)^2$ is not principal. If it were principal, then again we'd find $a + b\alpha$ with norm 4. Again, if $b \neq 0$, then the norm is too big, so we must have $b = 0$ and $a = \pm 2$. So, it suffices to show that $(2,\alpha)^2 \neq (2)$. But finally, comparing factorizations means that it suffices to show that $(2,\alpha) \neq (2,\alpha-1)$. This is true, since if they were equal, that ideal would contain $(\alpha) - (\alpha-1) = 1$, and so wouldn't be proper, whereas we know that it is prime. So, the class number is exactly 3.

Now, we use the same approach for $K = \mathbb{Q}(\sqrt{-47})$, $\mathscr{O}_K = \mathbb{Z}[\alpha]$ for $\alpha = (1+\sqrt{-47})/2$ of minimal polynomial $f(x) = x^2 - x + 12$ and discriminant $\Delta = -47$. The Minkowski bound is:

$$\frac{2!}{2^2}\left(\frac{4}{\pi}\right)^1 |-47|^{1/2} = (2/\pi)\sqrt{47} < 5$$

Now we seek integral ideals of norm 1, 2, 3, or 4. Again the only ideal of norm 1 is (1).

As above, when considered either modulo 2 or 3, we get that $f(x)$ splits as $x(x-1)$. So $(2) = (2,\alpha)(2,\alpha-1)$ and $(3) = (3,\alpha)(3,\alpha-1)$. Again considering norms gives

$$(\alpha) = (2,\alpha)^2(3,\alpha) \text{ and } (\alpha-1) = (2,\alpha-1)^2(3,\alpha-1)$$

So, the ideal classes represented by all of the above primes are in the cyclic subgroup generated by the class of $(2,\alpha)$. Now, if I is an integral ideal of norm 4, then each of its prime factors divides 2, so must be one of $(2,\alpha), (2,\alpha-1)$. Comparing norms shows that I is a product of exactly two such factors, so I is also a power of $(2,\alpha)$ in the ideal class group.

So, it suffices to find the order of $(2,\alpha)$ in the ideal class group. First, note:

$$\begin{aligned}
(2,\alpha)^2 &= (4, 2\alpha, \alpha^2) = (4, 2\alpha, \alpha - 12) = (4, \alpha) \\
(2,\alpha)^3 &= (8, 4\alpha, 2\alpha, \alpha^2) = (8, 2\alpha, \alpha - 12) = (8, \alpha - 4) \\
(2,\alpha)^5 &= (32, 8\alpha, 4\alpha - 16, \alpha^2 - 4\alpha) = (32, 8\alpha, 4\alpha - 16, -3\alpha - 12) = (\alpha + 4)
\end{aligned}$$

where the final equality follows from:

$$32 = (\alpha+4)(5-\alpha) \text{ and } 8\alpha = 8(\alpha+4) - 32 \text{ and } 4\alpha - 16 = 4(\alpha+4) - 32 \text{ and } -3\alpha - 12 = -3(\alpha+4)$$

So, the order of $(2, \alpha)$ divides 5. It finally remains to show that it isn't itself principal, for which it suffices to show that there is no element of norm 2. But

$$N(a+b\alpha) = (a+b\alpha)(a+b(1-\alpha)) = a^2 + ab + 12b^2 = \frac{1}{4}(2a+b)^2 + \frac{47}{4}b^2$$

For this to equal 2, we must have $b = 0$, lest it be too big, but then $a^2 = 2$, which has no integer solutions. So we're done and the ideal class group is cyclic of order 5. □

Exercise (4.5).

Proof. Let $I_1, \ldots, I_n$ be integral ideals of K that represent all ideal classes of K, so that the class group has order n. Then I_j^n is principal for each j, so we can find elements $\alpha_1, \ldots, \alpha_n \in K^\times$ with $I_j^n = (\alpha_j)$. Consider the extension $L = K(\alpha_1^{1/n}, \ldots, \alpha_n^{1/n})$ given by adjoining the n-th roots of these numbers.

First, note that $\alpha_j^{1/n} \in \mathscr{O}_L$ since they satisfy $T^n - \alpha_j$, and so are integral over $\mathscr{O}_K$. Second, note that

$$(\alpha_j^{1/n})^n = (\alpha_j) = I_j^n \mathscr{O}_L$$

But by uniqueness of factorization in $\mathscr{O}_L$, this gives $I_j\mathscr{O}_L = (\alpha_j^{1/n})$. Finally, if I is an arbitrary nonzero ideal of $\mathscr{O}_K$, then $I = \gamma I_j$ for some $\gamma \in K^\times$ and some j, whence $I\mathscr{O}_L = \gamma I_j \mathscr{O}_L = (\alpha_j^{1/n}\gamma)$ is principal. So, indeed, every ideal of $\mathscr{O}_K$ is principal in $\mathscr{O}_L$. □

Exercise (4.6).

Proof. By the invariant factor decomposition, we can find an integral basis for $\mathscr{O}_K$ of the form

$$1, \frac{f_1(\alpha)}{d_1}, \frac{f_2(\alpha)}{d_2}$$

where $f_i \in \mathbb{Z}[x]$ is monic of degree i and $1 \mid d_1 \mid d_2$ are the invariant factors of $\mathscr{O}_K$ over $\mathbb{Z}[\alpha]$. Thus, $|\mathscr{O}_K/\mathbb{Z}[\alpha]| = d_1 d_2$. We can compute the discriminant of α directly:

$$\Delta(\mathbb{Z}[\alpha]/\mathbb{Z}) = -N(3\alpha^2 - 1) = -N(3\alpha^3 - \alpha)/N(\alpha) = -N(2\alpha - 6)/(-2) = 4N(\alpha - 3) = -4f(3) = -4 \cdot 26 = -2^3 \cdot 13$$

But we also have $\Delta(\mathbb{Z}[\alpha]/\mathbb{Z}) = \Delta(\mathscr{O}_K/\mathbb{Z})|\mathscr{O}_K/\mathbb{Z}[\alpha]|^2 = \Delta(\mathscr{O}_K/\mathbb{Z})(d_1d_2)^2$. So, d_1^4 divides $-2^3 \cdot 13$ which forces $d_1 = 1$ and $d_2^2 \mid -2^3 \cdot 13$ which gives $d_2 = 1$ or $d_2 = 2$. Assume $d_2 = 2$ for contradiction. After adding multiples of previous basis elements if necessary, we can now assume our basis is of the form

$$1, \alpha, \frac{\alpha^2 + x\alpha + y}{2}$$

where $x, y \in \{0, 1\}$. In particular, these are all algebraic integers, so their traces should be in $\mathbb{Z}$. If $\alpha_1, \alpha_2, \alpha_3$ denote the roots of $x^3 - x + 1$ over a splitting field, then we get

$$T(\alpha^2) = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = (\alpha_1 + \alpha_2 + \alpha_3)^2 - 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = 0^2 - 2(-1) = 2$$

So, our last basis element has trace

$$\frac{2 + 0 + 3y}{2} = 1 + \frac{3}{2}y \in \mathbb{Z}$$

which forces $y = 0$. Similarly, we can take the norm of our last basis element to get

$$N\left(\frac{\alpha^2 + x\alpha}{2}\right) = \frac{1}{8}N(\alpha)N(\alpha + x) = -\frac{1}{4}f(-x) = \pm\frac{1}{2} \notin \mathbb{Z}$$

which is a contradiction. So, indeed $d_2 = 1$ and $\mathscr{O}_K = \mathbb{Z}[\alpha]$.

Now we'd like to compute the class number. Note that $x^3 - x + 2$ only has one real root. Indeed it strictly increases on the interval $(-\infty, -\sqrt{1/3})$, giving one root; strictly decreases on $(-\sqrt{1/3}, \sqrt{1/3})$ with a minimum of $f(\sqrt{1/3}) > 0$; and strictly increases on the rest of $(\sqrt{1/3}, \infty)$, thus remaining strictly positive. Hence K has two nonreal complex embeddings and so the Minkowski bound is:

$$\frac{3!}{3^3}\left(\frac{4}{\pi}\right)^1 |-2^3 13|^{1/2} \frac{16\sqrt{26}}{9\pi} < 3$$

So, if any ideal of $\mathscr{O}_K$ is not principal, it must have norm 2, in which case it must be a prime lying over 2. So, we consider the factorization of 2, which amounts to the factorization:

$$x^3 - x + 2 \equiv x(x-1)^2 \pmod 2$$

So, we get

$$(2) = (2, \alpha)(2, \alpha - 1)^2$$

in $\mathscr{O}_K$. But note that $N(\alpha) = -2$, so 2 is a multiple of α, showing that $(2, \alpha) = (\alpha)$ is principal. Similarly, $N(\alpha - 1) = -f(1) = -2$, so $(2, \alpha - 1) = (\alpha - 1)$ is also principal. So, there are no non-principal ideals of norm 2, and hence none at all. In other words, $\mathscr{O}_K$ has class number 1 and is a PID. □

Exercise (4.7).

Proof. Let $i = \sqrt{-1}$ and $\alpha = \frac{1+\sqrt{5}}{2}$. Note the minimal polynomial of α is $x^2 - x - 1$. We have that $\mathscr{O}_K \supseteq \mathbb{Z}[i, \alpha]$, and we can compute the discriminant Δ of the basis $\{1, \alpha, i, i\alpha\}$ directly:

$$\Delta = \det\begin{pmatrix} T(1) & T(\alpha) & T(i) & T(i\alpha) \\ T(\alpha) & T(\alpha+1) & T(i\alpha) & T(i(\alpha+1)) \\ T(i) & T(i\alpha) & T(-1) & T(-\alpha) \\ T(i\alpha) & T(i(\alpha+1)) & T(-\alpha) & T(-\alpha-1) \end{pmatrix} = \det\begin{pmatrix} 4 & 2 & 0 & 0 \\ 2 & 6 & 0 & 0 \\ 0 & 0 & -4 & -2 \\ 0 & 0 & -2 & -6 \end{pmatrix} = 20^2 = 2^4 5^2$$

So, we can conclude that $|\mathscr{O}_K/\mathbb{Z}[i, \alpha]| \mid 20$. Suppose $2 \mid |\mathscr{O}_K/\mathbb{Z}[i, \alpha]|$. Then we can find $u \in \mathscr{O}_K \setminus \mathbb{Z}[i, \alpha]$ of the form

$$u = \frac{a + b\alpha + ci + di\alpha}{2}$$

for $a, b, c, d \in \mathbb{Z}$. Let $\sigma : K \to K$ denote the automorphism with $\sqrt{5} \mapsto -\sqrt{5}$ and keeps i fixed. I.e. $\sigma(\alpha) = 1 - \alpha$ and $\sigma(i) = i$. Then $\sigma(u) \in \mathscr{O}_K$ as well, and

$$\sigma(u) = \frac{a + b(1-\alpha) + ci + di(1-\alpha)}{2}$$

But then the sum of these is $u + \sigma(u) = (a + b/2) + (c + d/2)i \in \mathscr{O}_K \cap \mathbb{Q}(i) = \mathscr{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$. So we must have b, d even. Then

$$u - \frac{b\alpha + di\alpha}{2} = \frac{a + ci}{2} \in \mathscr{O}_K \cap \mathbb{Q}(i) = \mathbb{Z}[i]$$

as well, giving that a, c are even. But then $u \in \mathbb{Z}[i, \alpha]$ contrary to assumption. So $|\mathscr{O}_K/\mathbb{Z}[i, \alpha]| \mid 5$. Similarly, if we assume that it equals 5, we can find

$$v = \frac{w + x\alpha + yi + zi\alpha}{5} \in \mathscr{O}_K \setminus \mathbb{Z}[i, \alpha]$$

for $w, x, y, z \in \mathbb{Z}$. If we let τ be the other generating automorphism with $\tau(\alpha) = \alpha$ and $\tau(i) = -i$, we get

$$v + \tau(v) = \frac{2w + 2x\alpha}{5} \in \mathscr{O}_K \cap \mathbb{Q}(\alpha) = \mathbb{Z}[\alpha]$$

and so both w, x are multiples of 5. Finally,

$$iv + \tau(iv) = \frac{-2y - 2z\alpha}{5} \in \mathbb{Z}[\alpha]$$

and so y, z are multiples of 5 as well. But this shows that $v \in \mathbb{Z}[i, \alpha]$ contrary to assumption and so we must have $\mathscr{O}_K = \mathbb{Z}[i, \alpha]$ after all.

This immediately shows that $2, 5$ ramify and no other primes, as they are precisely the primes dividing Δ. We know that $i(1-i)^2 = 2$, so we've already factorized somewhat.

$$\mathbb{Z}[i, \alpha]/(1-i) = \mathbb{Z}[\alpha][x]/(x^2+1, 1-x) = \mathbb{Z}[\alpha][x]/(2, x-1) = \mathbb{Z}[\alpha]/(2) = \mathbb{Z}[x]/(2, x^2-x-1) = \mathbb{F}_2[x]/(x^2+x+1) = \mathbb{F}_4$$

so that $(1-i)$ is a prime ideal. Thus, we've factored $(2) = (1-i)^2$ as ideals in $\mathcal{O}_K$, and indeed it ramifies with index 2. Similarly, $(2\alpha-1)^2 = (\sqrt{5})^2 = 5$, and

$$\mathbb{Z}[i,\alpha]/(2\alpha-1) = \mathbb{Z}[i][x]/(x^2-x-1, 2x-1) = \mathbb{Z}[i][x]/(5, x+2) = \mathbb{Z}[i]/(5) = \mathbb{F}_5[x]/(x^2+1)$$

However, this is not a domain since $x^2+1 = (x-2)(x+2)$ in $\mathbb{F}_5[x]$ is reducible. But this suggests the fix: we should enlarge our ideal to contain the preimage of $x+2$, namely $2+i$, and so we consider the ideal $(2\alpha-1, 2+i)$. We'll need the factorization so we compute:

$$(2\alpha-1,2+i)(2\alpha-1,2-i) = (4\alpha^2-4\alpha+1, (2\alpha-1)(2+i), (2\alpha-1)(2-i), 5) = (5, (2\alpha-1)(2+i), (2\alpha-1)(2-i)) = (2\alpha-1)$$

Indeed for the last equality "$\subseteq$" is obvious as each generator is a multiple of $2\alpha-1 = \sqrt{5}$, and for the reverse containment note that $5(2\alpha-1) - (2\alpha-1)(2+i) - (2\alpha-1)(2-i) = 2\alpha-1$. So, overall, we get the factorization

$$(5) = (2\alpha-1, 2+i)^2(2\alpha-1, 2-i)^2$$

Comparing norms gives $5^4 = N(\mathfrak{p})^2N(\mathfrak{q})^2$. We can see that $\mathfrak{p}$ is proper iff $\mathfrak{q}$ is by taking conjugates, so we cannot have $N(\mathfrak{p}) = 1$, hence $N(\mathfrak{p}) = N(\mathfrak{q}) = 5$, which also shows that they must be prime, thus giving that this is the complete factorization of 5 in $\mathcal{O}_K$, and that it is ramified of index 2.

Now, suppose that $\mathfrak{P}$ is a prime of $\mathcal{O}_K$ lying over the prime P of $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$ which itself lies over the prime (p) of $\mathbb{Z}$. Then $e(\mathfrak{P}/(p)) = e(\mathfrak{P}/P)e(P/(p))$. If $p \neq 2, 5$, then $e(\mathfrak{P}/(p)) = 1$, so $e(\mathfrak{P}/P) = 1$ and $\mathfrak{P}$ is unramified. If $p = 2, 5$, then $e(\mathfrak{P}/(p)) = 2$ as we've shown. But the discriminant of $\mathbb{Z}[\sqrt{-5}]$ is -20, so p ramifies here as well, giving $e(P/(p)) > 1$. On the other hand, the extension is of degree 2, so we must have $e(P/(p) \leq 2$, whence $e(P/(p)) = 2$ and $e(\mathfrak{P}/P) = 1$. So, in any case, we get that $\mathfrak{P}$ is unramified, and so the extension $K/\mathbb{Q}(\sqrt{-5})$ is totally unramified.

Finally, if we show that $\mathbb{Q}(\sqrt{-5})$ has class number 2, then we are done, as the Hilbert class field must contain K but is also a degree two extension of $\mathbb{Q}(\sqrt{-5})$, and so would equal K. But we know the ring of integers is $\mathbb{Z}[\sqrt{-5}]$ and the discriminant is $\Delta = -20$, so the Minkowski bound is

$$\frac{2!}{2^2}\left(\frac{4}{\pi}\right)^1 |-20|^{1/2} < 3$$

So the class group can be represented by (1) and primes lying over 2. For this we factor $x^2+5 \equiv (x+1)^2 \pmod 2$, so

$$(2) = (2, 1+\sqrt{-5})^2$$

in $\mathbb{Z}[\sqrt{-5}]$. So, we seek to show that $(2, 1+\sqrt{-5})$ is not principal, for which it suffices to show that $N(a+b\sqrt{-5}) = 2$ has no solutions. But this is obvious, as $a^2+5b^2 = 2$ has no integer solutions. So, indeed, the class number is 2 and we have exhibited its Hilbert class field. $\square$