Exercise (3.1).

Proof. Let R be a (unital, commutative) ring. Suppose first that every ideal is finitely generated. Then, consider an ascending sequence of ideals:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

Then, let

$$I = \bigcup_{n=1}^{\infty} I_n$$

First, note that I is an ideal. Indeed, if $x, y \in I$, then there are n, m with $x \in I_n$ and $y \in I_m$. Then $x, y \in I_{\max\{n,m\}}$, so $x + y \in I_{\max\{n,m\}} \subseteq I$. Further, if $r \in R$ is arbitrary, then $rx \in I_n \subseteq I$. Thus, by assumption, $I = (a_1, \ldots, a_n)$ for some elements $a_i \in R$. Then, for each i, $a_i \in I_{m_i}$ for some indices m_i, and then $a_i \in I_m \subseteq I$ for $m = \max\{m_1, \ldots, m_n\}$. But then $I = I_m$, and so the chain stabilizes: $I = I_m = I_{m+1} = I_{m+2} = \cdots$.

Second, assume that ascending chains stabilize. Let S be a nonempty set of ideals of R. Assume, for contradiction, that S has no maximal element. Then, we can inductively choose a sequence of ideals as follows: let $I_1 \in S$ be arbitrary. Then, since I_1 is not a maximal element of S, there is an ideal $I_2 \in S$ with $I_1 \subsetneq I_2$. Continue in this way: given $I_n \in S$, it is not maximal, so choose $I_{n+1} \in S$ with $I_n \subsetneq I_{n+1}$. But then we've constructed an ascending chain of ideals of R that does not stabilize, contrary to assumption.

Finally, suppose every nonempty collection of ideals has a maximal element. Let $I \subseteq R$ be an ideal, and let $S = \{(a_1, \ldots, a_n) \mid n \in \mathbb{N}, a_i \in I\}$ be the collection of finitely generated ideals contained in I. By assumption, this has a maximal element $(a_1, \ldots, a_n)$. But if $I \neq (a_1, \ldots, a_n)$, then there is some $a \in I \setminus (a_1, \ldots, a_n)$, giving that $(a_1, \ldots, a_n, a) \in S$ strictly contains $(a_1, \ldots, a_n)$. This would contradict maximality, and so we conclude $I = (a_1, \ldots, a_n)$ is finitely generated. □

Exercise (3.2).

Proof. Let R be a domain with $|R|$ finite, and let $\alpha \in R$ be nonzero. Consider the map $\mathbb{N} \to R$ given by $n \mapsto \alpha^n$. Since the codomain is finite, this map cannot be injective. So, there exist distinct $n, m \in \mathbb{N}$ with $\alpha^n = \alpha^m$. WLOG, $n < m$, whence we have

$$0 = \alpha^n(\alpha^{n-m} - 1)$$

But since R is a domain, we either get $\alpha = 0$ or $\alpha^{n-m} = 1$. The former is not true by assumption, and so $\alpha^{n-m} = 1$. So α is invertible and R is a field. □

Exercise (3.3).

Proof. Let G be generated (freely) by $e_1, \ldots, e_n \in G$. Then G/mG is generated by the images $e_i + mG$. Each has order m since $me_i \in mG$, and there are no further relations. For if

$$\sum_{i=1}^{n} a_i(e_i + mG) = mG$$

then $\sum a_i e_i \in mG$, and since these generate freely, each a_i must be a multiple of m. So, the sum is already zero. I.e. G/mG is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^n$ as claimed. □

Exercise (3.4).

Proof. As hinted, if $\alpha \in I$ is nonzero, then $\alpha R \subseteq I \subseteq R$, and so I is an abelian group contained in and containing a free abelian group of rank n. So I is also a free abelian group of rank n. □

Exercise (3.5).

Proof. The two remaining claims in the proof of [Lemma 2, Theorem 15] are that $\gamma \in K \setminus R$ and $\gamma A \subseteq R$. The first is clear, for if $\gamma \in R$, then $b = a\gamma \in (a)$, contrary to assumption. For the second, note that $b \in P_2 \cdots P_r$ and $A \subseteq P = P_1$. Hence $bA \subseteq P_1 \cdots P_r \subseteq aR$. So, $\gamma A \subseteq R$ as claimed. □

Exercise (3.6).

Proof. The only two gaps in the proof are:

- A is an ideal since it is clearly an R-submodule of K contained in R.
- $\gamma J \subseteq J$, since for $\beta \in J$, we have $\gamma\beta \in \gamma J \subseteq R$ and

$$\gamma\beta I \subseteq \gamma IJ = \gamma\alpha A \subseteq \alpha R$$

  so that $\gamma\beta \in J$ by definition.

□

Exercise (3.7).

Proof. If $I + J = R$, then there is $a \in I$, $b \in J$ with $a + b = 1$. Then, by the binomial theorem,

$$1 = 1^{n+m} = (a+b)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} a^i b^{n+m-i}$$

Each summand is either divisible by a^m and so is in I^m or else is divisible by b^n and so is in J^n. So we have $I^m + J^n = R$ as claimed. □

Exercise (3.8).

Proof.

(a) Suppose, for contradiction, that $(2, x) = (f)$ for some $f \in \mathbb{Z}[x]$. Then $2 = fg$ for some $g \in \mathbb{Z}[x]$, so that f has degree zero, i.e. $f \in \mathbb{Z}$. Then $f = \pm 1$ or $f = \pm 2$. We cannot have either of the first two, since then $(f) = \mathbb{Z}[x]$, but

$$\mathbb{Z}[x]/(f) = \mathbb{Z}[x]/(2, x) \cong \mathbb{F}_2$$

is nontrivial. But we also cannot have $f = \pm 2$ because $2 \nmid x$ in $\mathbb{Z}[x]$.

(b) As usual, we refer to the gcd of the coefficients of a polynomial as the content of that polynomial, and refer to any polynomial with content 1 as primitive. As suggested, we first show that the product of primitive polynomials is primitive. Indeed, suppose that $f = \sum_i a_i x^i$ and $g = \sum_j b_j x^j$ are both primitive. Now, let p be a prime, and note that there is some first coefficient of f that is not divisible by p, say a_n and similarly for g, i.e. b_m. But then the coefficient of x^{n+m} in fg is

$$\sum_{i=0}^{n+m} a_i b_{n+m-i}$$

and every term in this sum is divisible by p except the term $a_n b_m$, since it involves a_i for $i < n$ or b_j for $j < m$. So, this coefficient is not divisible by p. I.e. fg is primitive.

Now, for the general case, if m is the content of f and n is the content of g, then 1 is the content of $(f/m)(g/n)$, and so mn is the content of $fg = mn(f/m)(g/n)$.

(c) Contrapositively, suppose $f \in \mathbb{Z}[x]$ is reducible over $\mathbb{Q}$, so that $f = gh$ for nonconstant polynomials $g, h \in \mathbb{Q}[x]$. Then, we can clear denominators: for some $a, b \in \mathbb{Z}$ we get $ag, bh \in \mathbb{Z}[x]$. So,

$$abf = (ag)(bh)$$

i.e. this multiple of f is reducible in $\mathbb{Z}[x]$. Let t be the smallest positive integer such that tf is reducible in $\mathbb{Z}[x]$. If $t \neq 1$, then let p be a prime divisor of t, and note that if $tf = g'h'$, then p divides the content of tf, so it divides the product of the contents of g' and h'. So, it divides one of these, i.e. WLOG p divides the content of g', whence $g'/p \in \mathbb{Z}[x]$. But then $(t/p)f = (g'/p)h'$, contradicting the minimality of t. So we must have $t = 1$ so that $tf = f$ is reducible in $\mathbb{Z}[x]$.

(d) Since f is irreducible in $\mathbb{Z}[x]$, we've shown that f is irreducible in $\mathbb{Q}[x]$. So, $f \mid gh$ implies that $f \mid g$ or $f \mid h$ in $\mathbb{Q}[x]$. WLOG, suppose $f \mid g$, so that $g = fq$ for some $q \in \mathbb{Q}[x]$. As above, by clearing denominators, we can write $ag = f(aq)$ for some $a \in \mathbb{Z}$ such that $aq \in \mathbb{Z}[x]$. Then a divides the content of ag, which equals the content of aq, since f is primitive. So $q = (aq)/a \in \mathbb{Z}[x]$, so that $f \mid g$ in $\mathbb{Z}[x]$.

(e) To see that $\mathbb{Z}[x]$ is a UFD, we will show that every element can be written as a product of irreducibles and that all irreducibles are prime. The former is immediate, since this is true for any Noetherian ring ($\mathbb{Z}[x]$ is Noetherian since $\mathbb{Z}$ is, by an application of the Hilbert Basis Theorem). The latter is essentially what we've shown. Suppose f is irreducible and primitive. Then the above shows that if $f \mid gh$ then $f \mid g$ or $f \mid h$, so that f is prime. If f is not primitive, then $f = d(f/d)$, where d is the content of f. But since f is irreducible, we must have that d is a prime integer and that f/d is a unit, i.e. it is ± 1, so that f itself is $\pm p$ for a prime $p \in \mathbb{Z}$. In this case, $f = p$ is also prime in $\mathbb{Z}[x]$. So, in either case, we've shown that any irreducible is prime, and so $\mathbb{Z}[x]$ is a UFD.

□

Exercise (3.9).

Proof.

(a) Considering the union of all prime divisors of I and J in R, we can write

$$I = P_1^{a_1} \cdots P_n^{a_n} \qquad\qquad J = P_1^{b_1} \cdots P_n^{b_n}$$

for distinct primes P_i and $a_i, b_i \geq 0$. Then, each prime factors in S, so that

$$P_i S = Q_{i1}^{c_{i1}} \cdots Q_{it_i}^{c_{it_i}}$$

where each $c_{iu} > 0$ and as u varies, Q_{iu} enumerates the distinct primes lying over P_i. Further, for $i \neq j$ and any valid u, v, $Q_{iu} \neq Q_{jv}$ since they lie over distinct primes. Overall, this gives:

$$IS = \prod_{i=1}^{n} \prod_{u=1}^{t_i} Q_{iu}^{a_i c_{iu}}$$

and

$$JS = \prod_{i=1}^{n} \prod_{u=1}^{t_i} Q_{iu}^{b_i c_{iu}}$$

Since $IS \mid JS$ and these are all distinct primes, we must have $a_i c_{iu} \leq b_i c_{iu}$ for each i, u. Since each c_{iu} is positive, this gives $a_i \leq b_i$ for each i, and so $I \mid J$.

(b) As suggested, let $J = IS \cap R$. Then, if $x \in I \subseteq R$, then $x \in IS$ also, so $x \in J$, i.e. $I \subseteq J$, so $J \mid I$. But also clearly $JS \subseteq IS$, so $IS \mid JS$, and the previous gives $I \mid J$. Thus $I = J$, i.e. $I = IS \cap R$.

(c) I claim the following is necessary and sufficient for $I = (I \cap R)S$: for each prime P dividing $I \cap R$, there is an n such that for each prime Q of S lying over P, the exponent of Q in the factorization of I is precisely $ne(Q|P)$. Indeed, this is sufficient, for if this holds, then

$$I \cap R = P_1^{n_1} \cdots P_k^{n_k}$$

and then for each prime Q lying over P_i, the exponent of Q in the factorization of $(I \cap R)S$ is $n_i e(Q|P_i)$, which by assumption is the exponent of Q in the factorization of I. Conversely, suppose $I = (I \cap R)S$. Then, if P^n divides $I \cap R$ exactly (i.e. P^{n+1} does not divide $I \cap R$), then writing

$$P = Q_1^{e_1} \cdots Q_t^{e_t}$$

we get that $Q_i^{ne_i}$ exactly divides $(I \cap R)S$, and so the exponent of Q_i in I is exactly $ne_i = ne(Q_i|P)$ as claimed.

□

Exercise (3.10).

Proof. Let $R \subseteq S \subseteq T$ be number rings and let $U \subseteq T$ be prime. Let $Q = S \cap U$ and $P = R \cap Q$ be the corresponding primes lying under. Then QT can be written as a product where one of the factors is $U^{e(U|Q)}$, and PS can similarly be written as a product with one factor equal to $Q^{e(Q|P)}$. Substituting this in gives that $PT = (PS)T$ has a factor of $Q^{e(Q|P)}T = (QT)^{e(Q|P)}$, which has a factor of

$$(U^{e(U|Q)})^{e(Q|P)} = U^{e(U|Q)e(Q|P)}$$

and no higher power, so $e(U|P) = e(U|Q)e(Q|P)$.

Second, note that the inclusions $R \hookrightarrow S \hookrightarrow T$ composed with the quotient $T \to T/U$ induces ring homomorphisms:

$$R/P \to S/Q \to T/U$$

These are nontrivial morphisms and each ring is a field, so they are all injections. I.e. this is a tower of field extensions and the inertial degree is the degree of the extension, so that $f(U|P) = [T/U : R/P] = [T/U : S/Q][S/Q : R/P] = f(U|Q)f(Q|P)$. So, indeed both e, f are multiplicative. □

Exercise (3.11).

Proof. Let $\alpha \in I$. Then $\alpha R \subseteq I$, so $I \mid \alpha R$, so there is some nonzero ideal J with $\alpha R = IJ$. Then

$$\|I\|\|J\| = \|IJ\| = \|\alpha R\| = N^K(\alpha)$$

so that $\|I\| \mid N^K(\alpha)$ as claimed. If these are equal, then $[R : J] = \|J\| = 1$, so $J = R$. Then $\alpha R = IJ = IR = I$ as claimed. Conversely, if $\alpha R = I$, then clearly the two ideals have the same norm. □

Exercise (3.12).

Proof. We show both containments. First, note that

$$(5, \alpha + 2)(5, \alpha^2 + 3\alpha - 1) = (25, 5\alpha + 10, 5\alpha^2 + 15\alpha - 5, 5\alpha^2 + 5\alpha)$$

Clearly this is contained in $5S$ since each generator is. Conversely, this ideal contains

$$(5\alpha + 10)(2\alpha + 2) - 2(5\alpha^2 + 15\alpha - 5) - 25 = 5$$

and so it contains $5S$. So the two are equal.

Consider the map $\mathbb{Z}[x] \to \mathbb{F}_5[x]/(x^2 + 3x - 1)$ (that maps x and 1 to themselves). The kernel clearly contains 5 and $x^2 + 3x - 1$. If f is in the kernel, then by polynomial division we can write $f(x) = q(x)(x^2 + 3x - 1) + r(x)$ for $q, r \in \mathbb{Z}[x]$ and r of degree at most 1 since $x^2 + 3x - 1$ is monic. Then r is in the kernel, and factorizing it (since $\mathbb{Z}[x]$ is a UFD), we find that each prime factor of r is nonzero in the image except possibly 5. Since r is in the kernel, it must be divisible by 5, i.e. $f \in (x^2 + 3x - 1, 5)$, so this is precisely the kernel. I.e. we have an isomorphism:

$$\mathbb{Z}[x]/(5, x^2 + 3x - 1) \cong \mathbb{F}_5[x]/(x^2 + 3x - 1)$$

as claimed.

Consider the map $\mathbb{Z}[x] \to S/(5, \alpha^2 + 3\alpha - 1)$ that maps x to α. Then clearly 5 is in the kernel and $x^2 + 3x - 1 \mapsto \alpha^2 + 3\alpha - 1 = 0$ in the latter ring. So, this factors as a map

$$\mathbb{Z}[x]/(5, x^2 + 3x - 1) \to S/(5, \alpha^2 + 3\alpha - 1)$$

as claimed.

So, $S/(5, \alpha^2 + 3\alpha - 1)$ is (isomorphic to) a quotient of $\mathbb{F}_5[x]/(x^2 + 3x - 1)$. But $x^2 + 3x - 1$ is irreducible in this ring since it has no roots in $\mathbb{F}_5$. So $\mathbb{F}_5[x]/(x^2 + 3x - 1)$ is a field and so the only ideals are the zero and improper ideals, hence the only quotients are itself and the zero ring. So, we get that $(5, \alpha^2 + 3\alpha - 1) = S$ or $S/(\alpha^2 + 3\alpha - 1) \cong \mathbb{F}_{25}$.

Finally, from the first part, if $(5, \alpha^2 + 3\alpha - 1) = S$, then $5S = (5, \alpha + 2)S$. But then $\alpha + 2 \in 5S$, so that $(\alpha + 2)/5 \in S$, which isn't true by unique representation of elements in $\mathbb{Q}[\alpha]$. □

Exercise (3.13).

Proof. As with the previous, we define I and compute:

$$\begin{aligned}
I &= (23, \alpha - 10)^2(23, \alpha - 3) \\
&= (23^2, 23(\alpha - 10), \alpha^2 - 20\alpha + 100)(23, \alpha - 3) \\
&= (23^3, 23^2(\alpha - 10), 23(\alpha^2 - 20\alpha + 100), 23^2(\alpha - 3), 23(\alpha^2 - 13\alpha + 30), \alpha^3 - 23\alpha^2 + 160\alpha - 300) \\
&= (23^3, 23^2(\alpha - 10), 23(\alpha^2 - 20\alpha + 100), 23^2(\alpha - 3), 23(\alpha^2 - 13\alpha + 30), -23\alpha^2 + 161\alpha - 299) \\
&= (23^3, 23^2(\alpha - 10), 23(\alpha^2 - 20\alpha + 100), 23^2(\alpha - 3), 23(\alpha^2 - 13\alpha + 30), -23(\alpha^2 - 7\alpha + 13))
\end{aligned}$$

This is contained in $23S$ since each generator is a multiple of 23. Further, we have:

$$\det\begin{pmatrix} 1 & 1 & 1 \\ -20 & -13 & -7 \\ 100 & 30 & 13 \end{pmatrix} = 7 \cdot 43$$

which is nonzero in $\mathbb{F}_{23}$. So, by linear algebra there are $a, b, c \in \mathbb{Z}$ with

$$a(x^2 - 20x + 100) + b(x^2 - 13x + 30) + c(x^2 - 7x + 13) = 23r(x) + 1$$

for some polynomial $r \in \mathbb{Z}[x]$. Thus, $23^2 r(x) + 23 \in I$. We also have

$$23^2(\alpha - 3) - 23^2(\alpha - 10) = 23^2 \cdot 7 \in I$$

Since 23 and 7 are coprime (in $\mathbb{Z}$), there are $u, v \in \mathbb{Z}$ with $23u + 7v = 1$. Then, $23^3 \in I$, so

$$23^3 u + (23^2 \cdot 7)v = 23^2(23u + 7v) = 23^2 \in I$$

as well. Since $23^2 \in I$ and $23^2 r + 23 \in I$, we finally conclude $23 \in I$, as claimed. Thus finally we get $23S = I$.

We have $(23, \alpha - 10) + (23, \alpha - 3) = (23, \alpha - 10, \alpha - 3)$, so if we can show the latter is S, then they will indeed be coprime ideals. But the latter ideal contains

$$23u + (\alpha - 3)v - (\alpha - 10)v = 23u + 7v = 1$$

and so it is S. □

Exercise (3.14).

Proof. First, note that G acts on the set of primes lying over P. We've shown that this action is transitive; for a prime Q over P, let G_Q denote the stabilizer of Q. Thus, if Q, Q' are two primes lying over P, then there is some $\alpha \in G$ with $\alpha(Q) = Q'$, and so αG_Q is the set of automorphisms that map Q to Q'. But αG_Q and G_Q have the same size, as desired. Thus, if there are r primes lying over P, then $re(Q|P)f(Q|P) = n = r|G_Q|$, so $|G_Q| = e(Q|P)f(Q|P)$ as claimed.

Computing directly, we have, for a fixed Q over P:

$$\begin{aligned} P^{f(Q|P)} &= R \cap P^{f(Q|P)} S \\ &= R \cap \prod_{\substack{Q' \in \operatorname{Spec} S \\ Q \supseteq P}} (Q')^{e(Q'|P)f(Q|P)} \\ &= R \cap \prod_{\sigma \in G} \sigma(Q) \\ &= N_K^L(Q) \end{aligned}$$

since $f(Q|P) = f(Q'|P)$ for any Q' lying over P.

Note that if σ is an automorphism of L/K and I, J are ideals of S, then $\sigma(IJ) = \sigma(I)\sigma(J)$. So, let I be a nonzero ideal of S, so we can factorize it as $I = \prod_{i=1}^n Q_i$, where each Q_i is a prime lying over $P_i = Q_i \cap R$. So,

$$\prod_{\sigma \in G} \sigma(I) = \prod_{\sigma \in G} \prod_{i=1}^{n} \sigma(Q_i) = \prod_{i=1}^{n} P_i^{f(Q_i|P_i)} S$$

so the product is JS for $J = \prod_{i=1}^n P_i^{f(Q_i|P_i)}$. Then,

$$J = R \cap JS = R \cap \prod_{\sigma \in G} \sigma(I) = N_K^L(I)$$

and so

$$\prod_{\sigma \in G} \sigma(I) = JS = N_K^L(I) S$$

as claimed.

Directly, we have:

$$\begin{aligned}
N_K^L(IJ) &= R \cap N_K^L(IJ)S \\
&= R \cap \prod_{\sigma \in G} \sigma(IJ) \\
&= R \cap \prod_{\sigma \in G} \sigma(I)\sigma(J) \\
&= R \cap \left[\left(\prod_{\sigma \in G} \sigma(I)\right)\left(\prod_{\sigma \in G} \sigma(J)\right)\right] \\
&= \left[\left(R \cap \prod_{\sigma \in G} \sigma(I)\right)\left(R \cap \prod_{\sigma \in G} \sigma(J)\right)\right] \\
&= N_K^L(I)N_K^L(J)
\end{aligned}$$

as desired.

Again, we do this directly:

$$N_K^L(\alpha S) = R \cap \prod_{\sigma \in G} \sigma(\alpha S) = R \cap \left(\prod_{\sigma \in G} \sigma(\alpha)\right) S = R \cap N_K^L(\alpha)S = N_K^L(\alpha)R$$

as claimed. □

Exercise (3.15).

Proof. Note that it suffices to show the claim for primes, since both sides are multiplicative. So, let $R \subseteq S \subseteq T$ be the rings of integers in K, L, M, respectively, let $U \in \operatorname{Spec} T$, let $Q = U \cap S$, and let $P = Q \cap R$. Then,

$$N_K^L(N_L^M(U)) = N_K^L(Q^{f(U|Q)}) = N_K^L(Q)^{f(U|Q)} = (P^{f(Q|P)})^{f(U|Q)} = P^{f(U|Q)f(Q|P)} = P^{f(U|P)} = N_K^M(U)$$

as claimed.

As suggested, now let M be the normal closure of L/K. Then for $\alpha \in S$, and $n = [M : L]$, $N_L^M(\alpha) = \alpha^n$, so

$$N_K^L(\alpha^n S) = N_K^L(N_L^M(\alpha T)) = N_K^M(\alpha T) = N_K^M(\alpha)R = [N_K^L(\alpha)]^n R$$

using the result of the previous problem and the fact that M/L and M/K are normal. Since the norm is multiplicative and prime factorizations are unique, $N_K^L(\alpha S) = N_K^L(\alpha)R$ as claimed.

As suggested, note that if $P \in \operatorname{Spec} S$, then P lies over a rational prime $p \in \mathbb{Z}$, and

$$N_{\mathbb{Q}}^L(P) = (p\mathbb{Z})^{f(P|p)} = p^{f(P|p)}\mathbb{Z} = |S/P|\mathbb{Z} = \|P\|\mathbb{Z}$$

as claimed. Further, both sides are multiplicative, so this is now true for all ideals I of S. □

Exercise (3.16).

Proof. We have a map of ideals $I \mapsto N_K^L(I)$. To show that it induces a map of class groups, we show that it maps equivalent elements to equivalent elements. So, let A, B be nonzero ideals of S with nonzero elements $a, b \in S$ with $aA = bB$. Then,

$$N_K^L(a)N_K^L(A) = N_K^L(aA) = N_K^L(bB) = N_K^L(b)N_K^L(B)$$

and so $N_K^L(A)$ and $N_K^L(B)$ are equivalent.

For an ideal I, let $[I]$ denote the class of I in the class group. Then:

$$[R] = N_K^L([S]) = N_K^L([Q]^{d_Q}) = [N_K^L(Q)^{d_Q}] = [P^{f(Q|P)d_Q}]$$

so that $d_P \mid f(Q|P)d_Q$ as claimed. □

Exercise (3.17).

Proof. Throughout, let $S = \mathbb{Z}[\omega]$.

First, we have that $f(Q|2)$ is the multiplicative order of 2 mod 23, which is 11. Then, $f(Q|P)f(P|2) = f(Q|2) = 11$, and $f(P|2) \le [K : \mathbb{Q}] = 2$, so we must have $f(P|2) = 1$ and $f(Q|P) = 11$. Then, since $[L : K] = [L : \mathbb{Q}]/[K : \mathbb{Q}] = 22/2 = 11$, we get that $PS = Q$, since the sum of $e \cdot f$ over all primes lying over P gives 11. I.e. $Q = (2R + \theta R)S = 2S + \theta S$ as claimed.

We have:

$$P^3 = (8, 4\theta, 2\theta^2, \theta^3) = (8, 4\theta, 2\theta - 12, 5\theta + 6)$$

since $\theta^2 = \theta - 6$. This equation also gives:

$$(\theta - 2)^2 = \theta^2 - 4\theta + 4 = -3\theta - 2 = -3(\theta - 2) - 8$$

So, $\theta - 2$ divides 8. Then it also divides $4(\theta - 2) + 8 = 4\theta$, $2(\theta - 2) - 8 = 2\theta - 12$, and $5(\theta - 2) + 16 = 5\theta + 6$. Thus $P^3 \subseteq (\theta - 2)$.

Conversely, $\theta - 2 = (5\theta + 6) - (4\theta) - (8)$, so $\theta - 2 \in P^3$. Thus, the two ideals are equal, as claimed.

On the other hand, suppose that P is principal, generated by α. Then $P^3 = (\alpha^3) = (\theta - 2)$, and so

$$8 = |N_{\mathbb{Q}}^{K}(\theta - 2)| = \|P\| = |N_{\mathbb{Q}}^{K}(\alpha^3)| = |N_{\mathbb{Q}}^{K}(\alpha)|^3$$

and so $N_{\mathbb{Q}}^{K}(\alpha) = \pm 2$. But if $\alpha = a + b\theta$, then its norm is:

$$(a + b\theta)(a + b(1 - \theta)) = a^2 + ab + b^2(\theta - \theta^2) = a^2 + ab + 6b^2 = \frac{a^2 + 11b^2 + (a + b)^2}{2}$$

So, in order for this to be ± 2, we would need $a^2 + 11b^2 + (a + b)^2 = \pm 4$, which must actually be 4. This forces $b = 0$, else it would be too large, and so $2a^2 = 4$, which has no integer solutions. So, P is indeed not principal.

From the previous exercise, $3 = d_P \mid d_Q f(Q|P) = 11 d_Q$. So, $3 \mid d_Q$ and Q is not principal.

Suppose $2 = \alpha\beta$ for some nonunits $\alpha, \beta \in S$. Then, $(\alpha)(\beta) = 2S = QQ'$, where Q is as above and $Q' = (2, 1 - \theta)$ lies over the other prime $P' = (2, 1 - \theta$ over 2. But then comparing prime factorizations gives that (WLOG) $Q = (\alpha)$, contradicting the fact that Q is not principal. ☐

Exercise (3.18).

Proof. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K into $\mathbb{C}$. Then:

$$\begin{aligned}
\operatorname{disc}(r\alpha_1, \alpha_2, \ldots, \alpha_n) &= \det \begin{pmatrix} r\sigma_1(\alpha_1) & r\sigma_2(\alpha_1) & \cdots & r\sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}^2 \\
&= r^2 \det \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}^2 \\
&= r^2 \operatorname{disc}(\alpha_1, \ldots, \alpha_n)
\end{aligned}$$

as claimed.

Similarly, if $\beta = c_2\alpha_2 + \cdots + c_n\alpha_n$:

$$\begin{aligned}
\operatorname{disc}(\alpha_1+\beta,\alpha_2,\ldots,\alpha_n) &= \det\begin{pmatrix} \sigma_1(\alpha_1+\beta) & \sigma_2(\alpha_1+\beta) & \cdots & \sigma_n(\alpha_1+\beta) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}^2 \\
&= \left[\det\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} + \sum_{j=2}^n c_j \det\begin{pmatrix} \sigma_1(\alpha_j) & \sigma_2(\alpha_j) & \cdots & \sigma_n(\alpha_j) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}\right]^2 \\
&= \operatorname{disc}(\alpha_1,\ldots,\alpha_n)
\end{aligned}$$

since each term of the sum is zero, as it contains a repeated row.

□

Exercise (3.19).

Proof. As suggested, let $\overline{\alpha} \in R/P$ and $\overline{\beta} \in S/PS$ be the images of α, β under the quotient maps. Since S/PS is an R/P-vector space, the equation $\overline{\alpha}\overline{\beta} = 0$ implies that $\overline{\alpha} = 0$, so $\alpha \in P$, or else $\overline{\beta} = 0$, so $\beta \in PS$.

More directly, if $\alpha\beta \in PS$ and we assume $\beta \notin P$, then since P is maximal, $R\beta + P = R$, so we can find $r \in R$ and $p \in P$ with $r\beta + p = 1$. Then,

$$\alpha = r\alpha\beta + p\alpha \in PS$$

since both summands are.

Note that if $\beta_i \notin P$ for some i, then $\gamma = 1$ works trivially. So, we may assume $\beta_i \in P$ for each i, so that $\alpha\beta \in PS$. But $\alpha \notin PS$, so the previous argument gives $\beta \in P$ as well. Thus, $B = (\beta, \beta_1, \ldots, \beta_n) \subseteq P$. By a lemma from the chapter, there is some $\gamma \in K$ with $B\gamma \subseteq R$ but $B\gamma \not\subseteq P$. It is clear that $\beta\gamma \in R$ and $\beta_i\gamma \in R$ for each i. So, we need only show that it isn't the case that $\beta_i\gamma \in P$ for all P. Suppose this is the case; then

$$\alpha(\beta\gamma) = \sum_{i=1}^n \alpha_i(\beta_i\gamma) \in PS$$

and so the previous result again gives $\beta\gamma \in P$. But then $B\gamma \subseteq P$, contrary to assumption. So, $\beta_i\gamma \notin P$ for some i.

For the claim, we imitate the proof of theorem 24. Since P is ramified in S, the factorization of PS contains a repeated prime. Removing that prime, we get an ideal I of S such that $I \supsetneq PS$ and such that each prime lying over P divides I. Now, I contains PS properly, so choose $\alpha \in I \setminus PS$, and using the fact that the α_i form a basis, write:

$$\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n$$

for some $c_i \in K$. Clearing denominators gives:

$$\alpha\beta = \alpha_1\beta_1 + \cdots + \alpha_n\beta_n$$

for $\beta, \beta_i \in R$ and $c_i = \beta_i/\beta$. By the previous, after multiplying by an element $\gamma \in K$ if necessary, we may assume that not all $\beta_i \in P$, and after rearranging we may assume $\beta_1 \notin P$. Then, from a previous exercise, we have:

$$\operatorname{disc}_K^L(\alpha,\alpha_2,\ldots,\alpha_n) = \operatorname{disc}_K^L(\alpha_1\beta_1,\alpha_2,\ldots,\alpha_n) = \beta_1^2 \operatorname{disc}_K^L(\alpha_1,\ldots,\alpha_n)$$

So, to show that $\operatorname{disc}_K^L(\alpha_1,\ldots,\alpha_n) \in P$, it suffices to show that $d = \operatorname{disc}_K^L(\alpha,\alpha_2,\ldots,\alpha_n) \in P$, since P is prime and $\beta_1 \notin P$.

Let M be a normal extension of L/K, fix a prime Q of (the ring of integers of) M, and let σ be a K-embedding of L into $\mathbb{C}$. Then σ extends to an automorphism of M, and so $\sigma^{-1}(Q)$ is also a prime lying over P. So $\sigma^{-1}(Q) \cap S$ is a prime of S lying over P, which divides (and thus contains) I, and so $\alpha \in \sigma^{-1}(Q)$. This shows that $\sigma(\alpha) \in Q$ for each σ, and so expanding d as a determinant shows that $d \in Q$ as well. But we also have that $d \in R$, and so $d \in R \cap Q = P$ as desired. □

Exercise (3.20).

Proof. Let $f_i = f(Q_i|P)$, and write $B_i = \{\beta_{i1}, \dots, \beta_{if_i}\}$. Let

$$s = \sum_{i=1}^{r} \sum_{j=1}^{e_i} \sum_{k=1}^{f_i} c_{ijk} \alpha_{ij} \beta_{ik}$$

for some $c_{ijk} \in R$, and suppose $s \in P$. We'd like to show that each $c_{ijk} \in P$. Consider this equation mod Q_i. Then since $s \in P \subseteq PS \subseteq Q_i$:

$$0 \equiv s \equiv \sum_{k=1}^{f_i} c_{i1k} \alpha_{i1} \beta_{ik} = \alpha_{i1} \sum_{k=1}^{f_i} c_{i1k} \beta_{ik} \pmod{Q_i}$$

since $\alpha_{hj} \in Q_i$ for $h \neq i$ as well as for $h = i$ and $j > 1$. But $\alpha_{i1} \neq 0$ since it isn't in Q_i, so the sum must be zero. But β_{ik} is a basis for S/Q_i over R/P (as k varies), so we conclude $c_{i1k} \in P$ for all k. Since i was arbitrary, $c_{i1k} \in P$ for all i, k.

Now, suppose we've shown $c_{irk} \in P$ for all r less than some $j > 1$. Then we'll show $c_{ijk} \in P$ for all i, k. For this, consider s modulo Q_i^j. Then, again $s \in P \subseteq PS \subseteq Q_i^{e_i} \subseteq Q_i^j$, so:

$$0 \equiv s \equiv \sum_{k=1}^{f_i} c_{ijk} \alpha_{ij} \beta_{ik} = \alpha_{ij} \sum_{k=1} c_{ijk} \beta_{ik} \pmod{Q_i^j}$$

Now, $\alpha_{ij} \notin Q_i^j$, so we must have that the sum is in Q_i. Again using the fact that β_{ik} forms a basis gives $c_{ijk} \in P$ for all i, k. By induction $c_{ijk} \in P$ for all i, j, k, as claimed. □

Exercise (3.21).

Proof. As suggested, suppose $p \mid |S/G|$, so there is some $a \in S \setminus G$ such that $pa \in G$. I.e. we can write:

$$pa = c_1 \alpha_1 + \cdots + c_n \alpha_n$$

for some $c_i \in \mathbb{Z}$. But since the α_i are independent, we conclude that each $c_i \in p\mathbb{Z}$, i.e. $c_i = pd_i$ for some $d_i \in \mathbb{Z}$. Then

$$a = d_1 \alpha_1 + \cdots + d_n \alpha_n \in G$$

contrary to assumption.

Then,

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \operatorname{disc}(G) = |S/G|^2 \operatorname{disc}(S)$$

which is the claim, since $m = |S/G|^2$ is not divisible by p.

Now, let M be a normal extension of $L/\mathbb{Q}$ and let T be its ring of integers. Extend the K-embeddings of L into $\mathbb{C}$ to automorphisms $\sigma_1, \dots, \sigma_n$ of M. From the previous problem, we are considering the elements $\alpha_{ij}\beta_{ik}$. Then $\operatorname{disc}(\alpha_{ij}\beta_{ik}) = \det(A)^2$, where A is the matrix consisting of elements $\sigma_t(\alpha_{ij}\beta_{ik})$. Fix a prime U of T lying over Q_1 and let $e = e(U|P)$ be the common ramification index; we'd like to compute $v_U(\det(A))$, the power of U appearing in the factorization of $\det(A)T$. Since each automorphism permutes the primes in T, $v_U(\sigma(x))$ is at least as large as the smallest exponent occuring in the factorization of xT. Thus:

$$v_U(\sigma_t(\alpha_{ij}\beta_{ik})) \geq v_U(\sigma_t(\alpha_{ij})) \geq \min\left(\left\{\frac{e}{e_i}(j-1)\right\} \cup \left\{\frac{e}{e_h} N \mid h \neq i\right\}\right) = \frac{e}{e_i}(j-1)$$

as long as N is large enough.

Thus, when computing the valuation of $\det(A)$, we can factor out at least $U^{e(j-1)/e_i}$ from the column corresponding to $\alpha_{ij}\beta_{ik}$. Thus, we get:

$$v_U(\det(A)) \geq \sum_{i=1}^{r} \sum_{j=1}^{e_i} \sum_{k=1}^{f_i} \frac{e(j-1)}{e_i} = \frac{e}{2} \sum_{i=1}^{r} f_i(e_i - 1)$$

and so

$$v_p(\det(A)^2) = \frac{2}{e} v_U(\det(A)) \geq \sum_{i=1}^{r} f_i(e_i - 1) = k$$

as claimed. The first part of the problem gives that $p^k \mid \operatorname{disc}(S)$ as well, since $\det(A)^2 / \operatorname{disc}(S)$ is a p-free integer. □

Exercise (3.22).

Proof. Suppose $\alpha^5 - 2\alpha - 2 = 0$. Then

$$\operatorname{disc}(\alpha) = 5^5(-2)^4 + 4^4(-2)^5 = 2^4 \cdot 3 \cdot 13 \cdot 67$$

Let $R = \mathbb{Z}[\alpha]$ and S be the ring of integers in $\mathbb{Q}(\alpha)$. We know $R \subseteq S$ and

$$\operatorname{disc}(R) = \operatorname{disc}(S)|S/R|^2$$

So, we have that $|S/R|$ is a power of two, since the square of no other prime divides $\operatorname{disc}(R)$. So, finally, we seek the power of 2 dividing $\operatorname{disc}(S)$. The previous problem suggests studying the factorization of $2S$. But from 2.43, $\alpha + 1$ is a unit, and so

$$(\alpha S)^5 = \alpha^5 S = (2\alpha + 2)S = 2(\alpha + 1)S = 2S$$

So, the factorization of $2S$ is given by the factorization of αS raised to the fifth. But the exponents in the factorization of $2S$ sum to at most $n = 5$, so this must be the factorization itself. I.e. αS is the unique prime lying over 2 with $e = 5$ and $f = 1$. By the previous exercise, $\operatorname{disc}(S)$ is divisible by $2^{(5-1)\cdot 1} = 2^4$.

This completes the computation, showing that $|S/R| = 1$, i.e. $S = R = \mathbb{Z}[\alpha]$.

Now consider the case $\alpha^5 + 2\alpha^4 - 2 = 0$; we consider 2.44 now. Then,

$$\operatorname{disc}(\alpha) = -2^4 \cdot 971$$

So, as before, we consider $2S$. But

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

since $\alpha^4 - 1$ is a unit. So, this is the factorization, and the previous problem gives that if S is the ring of integers in $\mathbb{Q}(\alpha)$, then $\operatorname{disc}(S)$ is divisible by 2^4 as well. So,

$$|S/\mathbb{Z}[\alpha]|^2 = \operatorname{disc}(\alpha)/\operatorname{disc}(S) \mid 971$$

so that $S = \mathbb{Z}[\alpha]$ as before. □

Exercise (3.23).

Proof. We establish each of the missing parts. First, 3.2. We have:

$$(2, 1 + \sqrt{m})^2 = (4, 2 + 2\sqrt{m}, m + 1 + 2\sqrt{m})$$

This is contained in $2R$ since m is odd. Since $m \equiv 3 \pmod 4$, we have $m = 3 + 4k$ for some k, so this ideal also contains:

$$(m + 1 + 2\sqrt{m}) - (2 + 2\sqrt{m}) - k(4) = m - 1 - 4k = 2$$

So, it contains $2R$ and the two are equal.

For 3.3, we have $m = 8k + 1$ for some k, so:

$$\left(2, \frac{1+\sqrt{m}}{2}\right)\left(2, \frac{1-\sqrt{m}}{2}\right) = \left(4, 1 + \sqrt{m}, 1 - \sqrt{m}, \frac{1-m}{4}\right) = (4, 1 + \sqrt{m}, 1 - \sqrt{m}, -2k)$$

This is again clearly contained in $2R$ (since $(1 \pm \sqrt{m})/2 \in R$). But it also contains $(1+\sqrt{m}) + (1-\sqrt{m}) = 2$, so it contains $2R$.

Finally, for 3.5, we have $n^2 = m + kp$ for some k, so

$$(p, n + \sqrt{m})(p, n - \sqrt{m}) = (p^2, p(n + \sqrt{m}), p(n - \sqrt{m}), kp)$$

which is clearly contained in pR. Conversely, it contains

$$p(n + \sqrt{m}) + p(n - \sqrt{m}) = 2np$$

and so it contains $\gcd(2np, p^2) = p$, since $p \nmid 2n$ as p is an odd prime and $p \nmid m$. So it contains pR. □

Exercise (3.24).

Proof. Equivalently, P is totally ramified in L if there is a unique prime Q of S lying over P with inertial degree 1. Now, $Q \cap M$ is the unique prime of M lying over P since any prime of M lying over P must be contained in a prime of S lying over P. We then also have:

$$1 = f(Q \mid P) = f(Q \mid Q \cap M) f(Q \cap M \mid P)$$

and so $f(Q \cap M \mid P) = 1$. I.e. P is totally ramified in M.

Notice that $K \subseteq L \cap L' \subseteq L$, so by the previous part, P is totally ramified in $L \cap L'$. But since $K \subseteq L \cap L' \subseteq L'$, it is also unramified in $L \cap L'$. That is, if U is a prime of L' lying over $Q \cap L'$, then

$$1 = e(U \mid P) = e(U \mid Q \cap L') e(Q \cap L' \mid P)$$

and so

$$1 = e(Q \cap L' \mid P) = [L \cap L' : K]$$

so that $L \cap L' = K$ as claimed.

Let R denote the ring of integers in $\mathbb{Q}[\omega]$, where ω is a primitive mth root of unity. Recall that we computed $\operatorname{disc}(\omega)$, which did not require knowing the degree of the extension, and found that it divides a power of m. Hence, we know that a prime can only ramify if it divides m.

As suggested, if we first take $m = p^r$, then we've shown in 2.34 that $p = u(1-\omega)^{\varphi(m)}$ for some unit u. Thus, in this case, pR splits into at least $\varphi(m)$ factors, i.e. $[\mathbb{Q}(\omega) : \mathbb{Q}] \geq \varphi(m)$. But we know that each conjugate of ω must be a root of $(x^m - 1)/(x^{m/p} - 1)$, and so there are at most $m - m/p = p^r(1 - 1/p) = \varphi(m)$ of them. I.e. $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(m)$ in this case. We've also shown that p is totally ramified in this extension.

For the general case, suppose inductively that for a given m, we've shown that $[\mathbb{Q}(\zeta_t) : \mathbb{Q}] = \varphi(t)$ for $2 \leq t < m$ where ζ_t is a primitive tth root of unity. If m is a prime power, we're done, so assume it is not. Then, let p be a prime dividing m and factorize $m = p^r n$ with $r > 0$ and $p \nmid n$. Then, we have

$$\zeta_{p^r}, \zeta_n \in \mathbb{Q}(\omega)$$

and in fact they generate the full field extension over $\mathbb{Q}$. That is, $\mathbb{Q}(\omega)$ is the compositum of $\mathbb{Q}(\zeta_{p^r})$ and $\mathbb{Q}(\zeta_n)$. So,

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}][\mathbb{Q}(\zeta_n) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_{p^r}) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}]} = \frac{m}{[\mathbb{Q}(\zeta_{p^r}) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}]}$$

since the subextensions are Galois, and where the numerator comes from the inductive hypothesis. So, it suffices to show that $\mathbb{Q}(\zeta_{p^r}) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$. But this is immediate from the previous part of the problem; we have seen that p is totally ramified in $\mathbb{Q}(\zeta_{p^r})$ and unramified in $\mathbb{Q}(\zeta_n)$, and so the two fields intersect in $\mathbb{Q}$ as desired. ☐

Exercise (3.25).

Proof. ☐

Exercise (3.26).

Proof. Write $m = hk^2$ as in 2.41. Then from that exercise, $|R/\mathbb{Z}[\alpha]| = d_2 \mid 3k$. If $p^2 \nmid m$, then $p \nmid k$, and so $p \nmid |R/\mathbb{Z}[\alpha]|$, and the factorization of pR comes from the factorization of $x^3 - m \pmod{p}$.

Note $p \mid k$, $p^2 \nmid k$, and $p \nmid h$ in this case. Then:

$$\gamma^3 = \frac{\alpha^6}{k^3} = \frac{m^2}{k^3} = h^2 k$$

which is cubefree and not divisible by p^2. So, as in the first part, the factorization of pR is given by factoring $x^3 - h^2 k \equiv x^3 \pmod{p}$. So, we get our answer: $pR = (p, \gamma)^3$.

We have a $\mathbb{Z}$-basis for R given by $1, \alpha, f_2(\alpha)/d_2$ from 2.41, whence $|R/\mathbb{Z}[\alpha]| = d_2$. In the case $m \not\equiv \pm 1 \pmod{9}$, we get $d_2 = k$. We do further case work. If, modulo 9, m is either of 2 or 5, then $3 \nmid k$, so we can factorize directly. But $x^3 - m$ is irreducible over $\mathbb{F}_3$ since it is cubic with no roots, so we get that 3 is inert in R.

If m is either of 4 or 7 modulo 9, then $3 \nmid k$ still, but $x^3 - m \equiv (x-1)^3 \pmod{3}$. So 3 is totally ramified in this case, given by $3R = (3, \alpha - 1)^3$.

If m is either of $\pm 3 \pmod 9$, then $3 \mid m$, but $3 \nmid k$. So we can still factor the minimal polynomial of α and get $x^3 - m \equiv x^3 \pmod 3$, so $3R = (3, \alpha)^3$ in this case.

Finally, if $9 \mid m$, then $3 \mid k$ and $3 \nmid h$. So $h^2 k \equiv \pm 3 \pmod 9$ and we fall into the previous case when considering γ. That is, $3R = (3, \gamma)^3$ in this last case.

As suggested, consider $m \equiv \pm 1 \pmod 9$ and $m \not\equiv \pm 8 \pmod{27}$. Let $\beta = (\alpha \mp 1)^2/3$. Then, $\beta \in R$ and

$$\beta^2 = \frac{\alpha^4 \mp 4\alpha^3 + 6\alpha^2 \mp 4\alpha + 1}{9} = \frac{6\alpha^2 + (m \mp 4)\alpha + (1 \mp 4m)}{9}$$

Hence,

$$\begin{pmatrix} 1 \\ \beta \\ \beta^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & \mp 2/3 & 1/3 \\ (1 \mp 4m)/9 & (m \mp 4)/9 & 2/3 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix}$$

So, $\operatorname{disc}(\beta) = \det(A)^2 \operatorname{disc}(\alpha)$ for this matrix A. I.e.

$$\operatorname{disc}(\beta) = \left(\mp \frac{4}{9} - \frac{m \mp 4}{27} \right)^2 (-27m^2) = \frac{-(m \pm 8)^2 m^2}{27}$$

Note that this is divisible by 3 but no higher power of 3 since $v_3(m \pm 8) = 2$. So, 3 does not divide $|R/\mathbb{Z}[\beta]|$, and we can determine the splitting of $3R$ by factoring the minimal polynomial of β over $\mathbb{F}_3$. This is:

$$x^3 - x^2 + \frac{1 \pm 2m}{3} x - \frac{(m \mp 1)^2}{27} \equiv x^3 - x^2 = x^2(x-1) \pmod 3$$

since the linear and constant coefficients are divisible by 3. So, we finally get:

$$3R = (3, \beta)^2 (3, \beta - 1)$$

in this case.

We directly find:

$$\operatorname{disc}(R) = \frac{\operatorname{disc}(\alpha)}{|R/\mathbb{Z}[\alpha]|^2} = \frac{-27m^2}{(3k)^2} = -3h^2k^2$$

in this case. But $3 \nmid h, k$, so $9 \nmid \operatorname{disc}(R)$. On the other hand, if $3R = P^3$ for a prime P of R, then we would get that $v_3(\operatorname{disc}(R))$ is at least $\sum (e_i - 1) f_i = 2$. This isn't the case, so $3R$ isn't the cube of a prime. Since $3 \mid \operatorname{disc}(R)$, 3 is ramified, and so we only have the case $3R = P^2 Q$ for distinct primes P, Q. □

Exercise (3.27).

Proof. Notice

$$\operatorname{disc}(\alpha) = 4^4(-5)^5 + 5^5(-5)^4 = 3^2 \cdot 5^5 \cdot 41$$

So, for $p \neq 3, 5$, we get that $p \nmid |R/\mathbb{Z}[\alpha]|$, and we can find the factorization of pR by factoring $x^5 - 5x - 5 \pmod p$.

To handle $p = 5$, note:

$$(\alpha R)^5 = \alpha^5 R = 5(\alpha + 1)R = 5R$$

since $\alpha + 1$ is a unit. Indeed, if $\alpha_1, \ldots, \alpha_5$ are the conjugates of α, then,

$$f(x) = x^5 - 5x - 5 = \prod_i (x - \alpha_i)$$

So, evaluating at -1 gives:

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

So, $N(1 + \alpha) = 1$ and $1 + \alpha$ is a unit as claimed. But then αR is the unique prime lying over 5 and 5 is totally ramified. This aligns with the polynomial factorization since

$$x^5 - 5x - 5 \equiv x^5 \pmod 5$$

as claimed.

Finally, in the specific case of $p = 2$ we get:

$$x^5 - 5x - 5 \equiv (x^2 + x + 1)(x^3 + x^2 + 1) \pmod 2$$

and each of these is irreducible since they are at most degree 3 and have no roots in $\mathbb{F}_2$. So,

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

is the factorization. □

Exercise (3.28).

Proof. Notice

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0 = p^r \beta$$

since each coefficient is divisible by p^r. Further, taking norms gives:

$$\pm a_0^n = (\pm a_0)^n = N(\alpha)^n = N(\alpha^n) = N(p^r\beta) = p^{rn}N(\beta)$$

and so $p \nmid N(\beta)$ in $\mathbb{Z}$. But then if I is an ideal of R containing both β and p, then it contains $N(\beta)$ and p, and so it contains $\gcd(N(\beta), p) = 1$. So $I = R$ is the only ideal containing both; i.e. p and β are coprime in R.

But now factoring αR, $p^r R$, and βR gives that $p^r R$ is the nth power of an ideal. Namely, it is the subproduct of the factorization of $(\alpha R)^n$ consisting of those primes that contain p^r (and thus do not contain β).

If $\gcd(r, n) = 1$, then we can choose $a, b \in \mathbb{N}$ with $ar - bn = 1$. Then if $I^n = p^r R$ we get:

$$(I^a)^n = (I^n)^a = (p^r R)^a = p^{ar}R = p^{1+bn}R = (p^b R)^n \cdot pR$$

and so unique factorization gives that pR is an nth power as well. So, for any prime lying over p, the ramification index must be at least n, and so exactly n, giving that p is totally ramified.

By 4.21, $\operatorname{disc}(R)$ is divisible by

$$p^{\sum(e_i-1)f_i} = p^{(n-1)\cdot 1} = p^{n-1}$$

when $\gcd(r, n) = 1$. If $\gcd(n, r) = m > 1$, then the above calculations generalize to show $p^m R$ is an nth power, so that pR is a n/mth power. So, each prime lying over p has $e_i \geq n/m$. So, $v_p(\operatorname{disc}(R))$ is at least:

$$n - \sum f_i \geq n - \sum \frac{me_i}{n} f_i = n - \frac{m}{n} \sum e_i f_i = n - \frac{m}{n} \cdot n = n - m$$

I.e. $\operatorname{disc}(R)$ is divisible by p^{n-m}.

As in 2.43, let $f(x) = x^5 + ax + a$ for a squarefree and not ± 1 such that $4^4 a + 5^5$ is squarefree. We then have:

$$a^4(4^4 a + 5^5) = \operatorname{disc}(\alpha) = (d_3 d_4)^2 \operatorname{disc}(R)$$

and in that problem we've shown $d_3 d_4 \mid a^2$. Then for any prime divisor p of a, we have $r = 1$, so the above shows $\operatorname{disc}(R)$ is divisible by $p^{n-1} = p^4$. If $p \neq 5$, then $p \nmid 4^4 a + 5^5$, and if $p = 5$, then $p \mid 4^4 a + 5^5$, but $p^2 \nmid 4^4 a + 5^5$. So, applying v_p gives:

$$2v_p(d_3 d_4) + 4 = 4 + v_p(4^4 a + 5^5) \leq 5$$

and so $v_p(d_3 d_4) \leq 1/2$, but it's an integer and so $v_p(d_3 d_4) = 0$ for all prime divisors of $d_3 d_4$. In other words, we must have $d_3 d_4 = 1$ and so $d_3 = d_4 = 1$.

Similarly, in 2.44 we have $f(x) = x^5 + ax \pm a$ with a, $(4a)^4 \pm 5^5$ both squarefree, whence

$$a^4((4a)^4 \pm 5^5) = \operatorname{disc}(\alpha) = (d_3 d_4)^2 \operatorname{disc}(R)$$

and $d_3 d_4 \mid a^2$. But then for any prime divisor p of a, we have that $r = 1$, so $p^4 \mid \operatorname{disc}(R)$. As above, $p^4 \mid a^4$ and $p^2 \nmid ((4a)^4 \pm 5^5)$, so $p \nmid d_3 d_4$ and we get $d_3 = d_4 = 1$. □

Exercise (3.29).

Proof. Since $p \nmid |R/\mathbb{Z}[\alpha]|$, we can determine the splitting of p in R by the factorization of $f \pmod p$. But by assumption, f has a root $r \in \mathbb{F}_p$, so $x - r$ is a factor of $f(x) \pmod p$. Hence, $P = (p, \alpha - r)$ is a prime lying over p of inertial degree 1. I.e. we have an isomorphism $\mathbb{F}_p \cong R/P$. Composing with the quotient map gives the desired result:

$$R \to R/P \to \mathbb{F}_p$$

since under this map, $\alpha - r \mapsto 0$, i.e. $\alpha \mapsto r$.

Let α be a root of $f(x) = x^3 - x - 1$ and let $p = 5$. Then

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

which is not divisible by p. Hence $p \nmid |R/\mathbb{Z}[\alpha]|$, and $f(2) = 8 - 2 - 1 = 5 \equiv 0 \pmod p$, so f has a root in $\mathbb{F}_p$. So, we get a ring homomorphism $\varphi : R \to \mathbb{F}_5$ with $\alpha \mapsto 2$. Thus if $\beta \in R$ satisfied $\beta^2 = \alpha$, then

$$\varphi(\beta)^2 = \varphi(\beta^2) = \varphi(\alpha) = 2$$

but there is no element of $\mathbb{F}_5$ that squares to 2. So, $\sqrt{\alpha} \notin R$. Hence, it is also not in $\mathbb{Q}[\alpha]$, since if it were, it is also clearly integral, satisfying $f(x^3)$.

We use a similar approach for the other cases. Let α again be a root of $f(x) = x^3 - x - 1$ and now let $p = 7$. Then p still does not divide the discriminant -23, and $f(-2) = (-8) - (-2) - 1 = -7 \equiv 0 \pmod p$. So, we get a morphism $R \to \mathbb{F}_7$ with $\alpha \mapsto -2$. But since -2 is not a cube in $\mathbb{F}_7$, we cannot have $\sqrt[3]{\alpha} \in R$. Similarly, there is no solution to $t^2 + 2 = -2$ in $\mathbb{F}_7$, and so $\sqrt{\alpha - 2} \notin R$.

Finally, let α be a root of $f(x) = x^5 + 2x - 2$ and let $R = \mathbb{A} \cap \mathbb{Q}[\alpha]$. Then, f is irreducible by Eisenstein's criterion, and

$$\text{disc}(\alpha) = 4^4(2)^5 + 5^5(-2)^4$$

Note that this is not divisible by $p = 5$ since the second term is but the first term is not. Also note that $f(-1) = -1 - 2 - 2 = -5 \equiv 0 \pmod p$. So, we get a map $\varphi : R \to \mathbb{F}_5$ with $\alpha \mapsto -1$. Now, suppose there are $x, y, z \in R$ with $x^4 + y^4 + z^4 = \alpha$. Then,

$$-1 = \varphi(\alpha) = \varphi(x^4 + y^4 + z^4) = \varphi(x)^4 + \varphi(y)^4 + \varphi(z)^4$$

But in $\mathbb{F}_5$, fourth powers are either zero or one, so the sum on the right is one of $\{0, 1, 2, 3\}$, none of which are $-1 \pmod 5$. This is a contradiction, so there are no such x, y, z. ☐

Exercise (3.30).

Proof. As suggested, first consider the case when $f(0) = 1$. Then, suppose that f only has a root mod p for primes in a finite set P. Note that $f(x) = \pm 1$ only has finitely many roots since f is nonconstant. So, we can choose m to be a multiple of the product of the primes in P, such that $f(m) \neq \pm 1$ and note that

$$f(m) = a_n m^n + a_{n-1} m^n + \cdots + a_1 m + 1$$

This has a prime divisor p since it is neither ± 1, and so $p \in P$ since $f(m) \equiv 0 \pmod p$. But then $p \mid m$, and so $f(m) \equiv 1 \pmod p$, which is a contradiction. So there is no such finite set.

More generally, if $f(0)$ is not necessarily 1, let $g(x) = f(xf(0))/f(0)$. Note that this is also a polynomial with integer coefficients since each coefficient is divisible by $f(0)$ when f is evaluated at $xf(0)$. But $g(0) = f(0)/f(0) = 1$, so by the above, g has a root for infinitely many p. For each such p, if t is a root, then $tf(0)$ is a root of f mod that prime, so f also has roots mod infinitely many primes.

Now, let K be a number field, so there is some primitive element α with $K = \mathbb{Q}[\alpha]$. Let $R = K \cap \mathbb{A}$ be the ring of integers, and let f be the minimal polynomial of α over $\mathbb{Z}$. Then, by the above, there are infinitely many primes p such that f has a root mod p. Of these, at most finitely many divide $|R/\mathbb{Z}[\alpha]|$: disregard them. Now, for each remaining prime p, we have that the factorization of f over $\mathbb{F}_p$ has a linear factor, corresponding to a prime P of R lying over p with $f(P|p) = 1$, as desired.

Fix m, and let $\omega = e^{2\pi i/m}$. Then, from the above, there are infinitely many primes of $\mathbb{Z}[\omega]$ with inertial degree 1 over the corresponding prime of $\mathbb{Z}$. Of these, finitely many divide m: again, disregard them. For each remaining prime P lying over p, we also know that $f(P|p)$ is the multiplicative order of p modulo m. So, the fact that this equals 1 implies that $p \equiv 1 \pmod m$

as desired.

Let M be the normal closure of L/K, and let R, S, T be the rings of integers of K, L, M, respectively. By the above, there are infinitely primes U of M such that $f(U|p) = 1$, where p is the prime of $\mathbb{Z}$ lying under U. Of these, only finitely many are ramified (those that divide the discriminant), which we disregard. Thus, for each such U, we also have $e(U|p) = 1$. Since M is Galois over $\mathbb{Q}$, we also have that

$$pT = U_1 \cdots U_r$$

splits as the product of r primes, one of which is U, such that they all have the same inertial degrees and ramification indices. That is, $e(U_i|p) = f(U_i|p) = 1$ for each i, and so by counting, we see that there must be $r = [M : \mathbb{Q}]$ of them.

Now, let $P = U \cap R$ be the prime lying under U in R. We have that

$$PS = Q_1 \cdots Q_t$$

is the product of primes of S, each of which lies under some U_i. But this implies that $f(Q_i|P) = e(Q_i|P) = 1$ since these quantities are multiplicative in towers. Hence we must have $t = [L : K]$ and we conclude that each such P splits completely as claimed. Since each P lies over a different prime $p \in \mathbb{Z}$, we conclude that we indeed have infinitely many of them.

Finally, let f, R be as stated. Let $K = \mathrm{Frac}(R)$ be the field of fractions, let $L = K[x]/(f) = K[\alpha]$ be the field extension given by adjoining the root α of f, and let S be the ring of integers in L. By the above, there are infinitely many primes P of R that split completely in S. Of these, finitely many lie over a prime of $\mathbb{Z}$ that divides $|S/R[\alpha]|$, which we disregard. For the remaining primes, we can determine the splitting of PS by the factorization of f in $(R/P)[x]$. Since we already know PS splits completely, we conclude that f splits completely (into linear factors) mod P, as claimed. ☐

Exercise (3.31).

Proof. Note that a fractional ideal is an R-submodule of K. The product as defined is then the submodule of K generated by all products of elements in each submodule, which gives a definition independent of representatives.

Clearly $II^{-1} \subseteq R$ since each product xy with $x \in I$ and $y \in I^{-1}$ satisfies $xy \in R$. So, II^{-1} is an ideal of R. Assume, for sake of contradiction, that II^{-1} is a proper ideal. Then there is some $\gamma \in K - R$ such that $\gamma II^{-1} \subseteq R$. Then $\gamma I^{-1} \subseteq I^{-1}$. By considering the determinant of the matrix describing the multiplication by γ map, we conclude that γ is integral over R, but since R is normal, this implies that $\gamma \in R$, furnishing our contradiction. Hence, the fractional ideals of R form a group, with R as the identity element.

Let $(x/y)I$ be a fractional ideal for I an ideal of R and $x, y \in R$. Then we can factorize the ideals xR, yR, I into products of primes, and the factorization of the fractional ideal is clear.

Let $G = \{\alpha R \mid \alpha \in K^\times\}$ denote the free abelian group of principal fractional ideals. We have a group homomorphism $K^\times \to G$ given by $\alpha \mapsto \alpha R$. An element α is in the kernel iff $\alpha R = R$ iff $\alpha \in R^\times$. Hence, we get that $G \cong K^\times / R^\times$ is the multiplicative group of K mod units in R.

Note that if R is a PID then the set of nonzero principal ideals is the set of all nonzero ideals, which is a free abelian semigroup since R is Dedekind. Conversely, suppose R is a Dedekind domain with the nonzero principal ideals forming a free abelian semigroup. Let B be a basis.

We would like to show that R is a PID, for which it suffices to show that R is a UFD since R is Dedekind. Since R is Noetherian, the only thing to check is the uniqueness. That is, suppose

$$x_1 \cdots x_n = y_1 \cdots y_m$$

for irreducibles $x_i, y_i \in R$. I claim that each $x_iR, y_iR \in B$. Indeed, for $t = x_i$ or $t = y_i$, we can, by assumption, write

$$tR = (z_1R) \cdots (z_rR)$$

for some principal ideals $z_iR \in B$, not necessarily distinct. WLOG, we may assume that each z_iR is a proper ideal, else we omit it. But then $t = uz_1 \cdots z_r$ for a unit u, and by irreducibility, we must have $r = 1$ and $t = uz_1$, whence $tR = z_1R \in B$. Thus, the expressions

$$\prod_i x_iR = \prod_j y_jR$$

are the unique factorization of these principal ideals relative to the basis B. Hence, they must agree, i.e. $n = m$ and $x_iR = y_iR$ after rearranging. That is, $x_i = u_iy_i$ for units u_i for each i, which completes the proof that R is a UFD.

By assumption, each fractional ideal in G is of the form αI for $\alpha \in K^\times$ and I a nonzero ideal. Let C denote that ideal class group of R. Consider the map $\varphi : G \to C$ defined by:

$$\alpha I \mapsto [I]$$

First, we need to show that this is well-defined. Indeed, the same fractional ideal can have different representatives. Suppose $(x/y)I = (x'/y')I'$ for ideals I, I' and $x, y, x', y' \in R$. But then $xy'I = x'yI'$, and so $I \sim I'$, i.e. $[I] = [I']$. It is also clear that φ is a group homomorphism, for

$$\varphi((\alpha I)(\beta J)) = \varphi(\alpha\beta IJ) = [IJ] = [I][J] = \varphi(\alpha I)\varphi(\beta J)$$

To finish the proof, we will show φ is surjective with kernel H. For the first, note that each ideal class $[I]$ has a representative I, which is the image of $1I$. For the latter, note that a principal fractional ideal is of the form αR, which maps to $[R]$, the identity. Conversely, if $\varphi(\alpha I) = [R]$, then $[I] = [R]$, so $xI = yR$, whence $I = (y/x)R$ is principal. So, $C \cong G/H$ with isomorphism φ.

Finally, note that R is Noetherian so if αI is an arbitrary fractional ideal, then $I = \sum_{i=1}^r x_1 R$ for some $x_i \in R$, whence $\alpha I = \sum_{i=1}^r \alpha x_i R$ is finitely generated as an R-module. Conversely, suppose that $M \subseteq K$ is a nonzero finitely generated R-module. That is,

$$M = \sum_{i=1}^r \alpha_i R$$

for some $\alpha_i \in R$. Let y be the product of the denominators of the α_i, so that $y\alpha_i \in R$ for each i. Then,

$$M = \sum_{i=1}^r \frac{y\alpha_i}{y} R = \frac{1}{y}\left(\sum_{i=1}^r y\alpha_i R\right)$$

and the parenthesized expression is an R-submodule of R, i.e. an ideal. So $M = (1/y)I$ is a fractional ideal. □

Exercise (3.32).

Proof. Since J is a fractional ideal, we can write it as αH for some ideal H of R and some $\alpha \in K^\times$. Then,

$$J/(IJ) = (\alpha H)/(\alpha IH) \cong H/(IH)$$

via the multiplication by α, α^{-1} maps. But then,

$$|J/(IJ)| = |H/(IH)| = |(R/(IH))/(R/H)| = \frac{|R/(IH)|}{|R/H|} = \frac{\|IH\|}{\|H\|} = \frac{\|I\|\|H\|}{\|H\|} = \|I\| = |R/I|$$

as claimed. □

Exercise (3.33).

Proof. Note that both A^{-1} and A^* are clearly additive groups. Suppose that $\alpha \in A^{-1}$ and $s \in S$. Then $s\alpha A \subseteq sS \subseteq S$, so $s\alpha \in A^{-1}$. So A^{-1} is further an S-module. For $\alpha \in A^*$ and $r \in R$,

$$\mathrm{Tr}_K^L(r\alpha A) = r\,\mathrm{Tr}_K^L(\alpha A) \subseteq R$$

So $r\alpha \in A^*$ and A^* is an R-module. Finally, if $\alpha \in A^{-1}$, then

$$\mathrm{Tr}_K^L(\alpha A) \subseteq \mathrm{Tr}_K^L(S) = R$$

so that $\alpha \in A^*$.

First, suppose that A is a fractional ideal. Then it's an S-module, so $SA = A$. Further, there is some $x/y \in L$ and ideal I of S with $A = (x/y)I$. But then $yA = xI \subseteq S$, so $y \in A^{-1}$ shows that $A^{-1} \neq \{0\}$. Conversely, suppose that $SA = A$ and $A^{-1} \neq \{0\}$. Let $y \neq 0$ be in A^{-1}. Then $yA \subseteq S$ and is an S-module since $(yA)S = y(AS) = yA$, so yA is an ideal of S. But then $A = (1/y)(yA)$ is a fractional ideal.

Suppose $A \subseteq B$. If $\alpha \in B^{-1}$, then $\alpha A \subseteq \alpha B \subseteq S$, so $\alpha \in A^{-1}$ and $A^{-1} \supseteq B^{-1}$. If $\alpha \in B^*$, then $\mathrm{Tr}_K^L(\alpha A) \subseteq \mathrm{Tr}_K^L(\alpha B) \subseteq R$, so $\alpha \in A^*$ and $A^* \supseteq B^*$.

From the previous, we have that $A^{-1} \subseteq A^*$, so $\operatorname{diff} A = (A^*)^{-1} \subseteq (A^{-1})^{-1}$ as claimed.

We've noted that the fractional ideals form a group, with I^{-1} being the inverse of I under this group operation, and so $(I^{-1})^{-1} = I$.

Hence, for a fractional ideal I, we have $\operatorname{diff} I \subseteq (I^{-1})^{-1} = I$ as desired.

The next two facts follow from a unified fact: if $\operatorname{diff} A$ is contained in a fractional ideal J, then it is a fractional ideal. Indeed $(\operatorname{diff} A)^{-1} \supseteq J^{-1} \neq \{0\}$, so it suffices to show $S(\operatorname{diff} A) = \operatorname{diff} A$, and since $1 \in S$, it further suffices to show that $S(\operatorname{diff} A) \subseteq \operatorname{diff} A$. But note that $\operatorname{diff} A = (A^*)^{-1}$, and we've already noted that the inverse of any abelian subgroup of L is an S-module, so $\operatorname{diff} A$ is a fractional ideal.

To see how this lemma implies both of the claims, note that $\operatorname{diff} I \subseteq I$ exhibits $\operatorname{diff} I$ as a subset of a fractional ideal, so by the lemma $\operatorname{diff} I$ is a fractional ideal. Then, if $A \subseteq I$, then $A^* \supseteq I^*$, and $\operatorname{diff} A = (A^*)^{-1} \subseteq (I^*)^{-1} = \operatorname{diff} I$. But we've just shown that $\operatorname{diff} I$ is a fractional ideal, so $\operatorname{diff} A$ is contained in a fractional ideal and hence is also itself a fractional ideal.

Then □

Exercise (3.34).

Proof. □

Exercise (3.35).

Proof. □

Exercise (3.36).

Proof. □

Exercise (3.37).

Proof. □

Exercise (3.38).

Proof. □

Exercise (3.39).

Proof. □

Exercise (3.40).

Proof. □