Chapter 4

Factoring of Prime Ideals in Extensions

4.1 Lifting of Prime Ideals

Recall the basic $AKLB$ setup: A is a Dedekind domain with fraction field K, L is a finite, separable extension of K of degree n, and B is the integral closure of A in L. If $A = \mathbb{Z}$, then $K = \mathbb{Q}$, L is a number field, and B is the ring of algebraic integers of L.

4.1.1 Definitions and Comments

Let P be a nonzero prime ideal of A. The *lifting* (also called the *extension*) of P to B is the ideal PB. Although PB need not be a prime ideal of B, we can use the fact that B is a Dedekind domain [see (3.1.3)] and the unique factorization theorem (3.3.1) to write

$$PB = \prod_{i=1}^{g} P_i^{e_i}$$

where the P_i are distinct prime ideals of B and the e_i are positive integers [see (3.3.2)].

On the other hand, we can start with a nonzero prime ideal Q of B and form a prime ideal of A via

$$P = Q \cap A.$$

We say that Q *lies over* P, or that P is the *contraction* of Q to A.

Now suppose that we start with a nonzero prime ideal P of A and lift it to B. We will show that the prime ideals $P_1, \ldots, P_g$ that appear in the prime factorization of PB are precisely the prime ideals of B that lie over P.

4.1.2 Proposition

Let Q be a nonzero prime ideal of B. Then Q appears in the prime factorization of PB if and only if $Q \cap A = P$.

Proof. If $Q \cap A = P$, then $P \subseteq Q$, hence $PB \subseteq Q$ because Q is an ideal. By (3.3.5), Q divides PB. Conversely, assume that Q divides, hence contains, PB. Then

$$P = P \cap A \subseteq PB \cap A \subseteq Q \cap A.$$

But in a Dedekind domain, every nonzero prime ideal is maximal, so $P = Q \cap A$. ♣

4.1.3 Ramification and Relative Degree

If we lift P to B and factor PB as $\prod_{i=1}^{g} P_i^{e_i}$, the positive integer e_i is called the *ramification index* of P_i over P (or over A). We say that P *ramifies* in B (or in L) if $e_i > 1$ for at least one i. We will prove in a moment that B/P_i is a finite extension of the field A/P. The degree f_i of this extension is called the *relative degree* (or the *residue class degree*, or the *inertial degree*) of P_i over P (or over A).

4.1.4 Proposition

We can identify A/P with a subfield of B/P_i, and B/P_i is a finite extension of A/P.

Proof. The map from A/P to B/P_i given by $a + P \to a + P_i$ is well-defined and injective, because $P = P_i \cap A$, and it is a homomorphism by direct verification. By (3.1.2), B is a finitely generated A-module, hence B/P_i is a finitely generated A/P-module, that is, a finite-dimensional vector space over A/P. ♣

4.1.5 Remarks

The same argument, with P_i replaced by PB, shows that B/PB is a finitely generated A/P-algebra, in particular, a finite-dimensional vector space over A/P. We will denote the dimension of this vector space by $[B/PB : A/P]$.

The numbers e_i and f_i are connected by an important identity, which does not seem to have a name in the literature. We will therefore christen it as follows.

4.1.6 Ram-Rel Identity

$$\sum_{i=1}^{g} e_i f_i = [B/PB : A/P] = n.$$

Proof. To prove the first equality, consider the chain of ideals

$$\begin{aligned} B &\supseteq P_1 \supseteq P_1^2 \supseteq \cdots \supseteq P_1^{e_1} \\ &\supseteq P_1^{e_1} P_2 \supseteq P_1^{e_1} P_2^2 \supseteq \cdots \supseteq P_1^{e_1} P_2^{e_2} \\ &\supseteq \cdots \supseteq P_1^{e_1} \cdots P_g^{e_g} = PB. \end{aligned}$$

By unique factorization, there can be no ideals between consecutive terms in the sequence. (Any such ideal would contain, hence divide, PB.) Thus the quotient $\beta/\beta P_i$ of any two

consecutive terms is a one-dimensional vector space over B/P_i, as there are no nontrivial proper subspaces. (It is a vector space over this field because it is annihilated by P_i.) But, with notation as in (4.1.5), $[B/P_i : A/P] = f_i$, so $[\beta/\beta P_i : A/P] = f_i$. For each i, we have exactly e_i consecutive quotients, each of dimension f_i over A/P. Consequently, $[B/PB : A/P] = \sum_{i=1}^{g} e_i f_i$, as claimed.

To prove the second equality, we first assume that B is a free A-module of rank n. By (2.3.8), this covers the case where A is a PID, in particular, when L is a number field. If $x_1, \ldots, x_n$ is a basis for B over A, we can reduce mod PB to produce a basis for B/PB over A/P, and the result follows. Explicitly, suppose $\sum_{i=1}^{n}(a_i+P)(x_i+PB) = 0$ in B/PB. Then $\sum_{i=1}^{n} a_i x_i$ belongs to PB, hence can be written as $\sum_j b_j y_j$ with $b_j \in B, y_j \in P$. Since $b_j = \sum_k c_{jk} x_k$ with $c_{jk} \in A$, we have $a_k = \sum_j c_{jk} y_j \in P$ for all k.

The general case is handled by localization. Let $S = A\backslash P$, $A' = S^{-1}A, B' = S^{-1}B$. By (1.2.6), (1.2.9), and the Dedekind property (every nonzero prime ideal of A is maximal), it follows that A' has exactly one nonzero prime ideal, namely $P' = PA'$. Moreover, P' is principal, so A' is a *discrete valuation ring*, that is, a local PID that is not a field. [By unique factorization, we can choose an element $a \in P'\backslash(P')^2$, so $(a) \subseteq P'$ but $(a) \not\subseteq (P')^2$. Since the only nonzero ideals of A' are powers of P' (unique factorization again), we have $(a) = P'$.] Now B is the integral closure of A in L, so B' is the integral closure of A' in $S^{-1}L = L$. [The idea is that we can go back and forth between an equation of integral dependence for $b \in B$ and an equation of integral dependence for $b/s \in B'$ either by introducing or clearing denominators.] We have now reduced to the PID case already analyzed, and $[B'/PB' : A'/PA'] = n$.

Now $PB = \prod_{i=1}^{g} P_i^{e_i}$, and P_i is a nonzero prime ideal of B not meeting S. [If $y \in P_i \cap S$, then $y \in P_i \cap A = P$ by (4.1.2). Thus $y \in P \cap S$, a contradiction.] By the basic correspondence (1.2.6), we have the factorization $PB' = \prod_{i=1}^{g}(P_iB')^{e_i}$. By the PID case,

$$n = [B'/PB' : A'/PA'] = \sum_{i=1}^{g} e_i [B'/P_iB' : A'/PA'].$$

We are finished if we can show that $B'/P_iB' \cong B/P_i$ and $A'/PA' \cong A/P$. The statement of the appropriate lemma, and the proof in outline form, are given in the exercises. ♣

Problems For Section 4.1

We will fill in the gap at the end of the proof of the ram-rel identity. Let S be a multiplicative subset of the integral domain A, and let $\mathcal{M}$ be a maximal ideal of A disjoint from S. Consider the composite map $A \to S^{-1}A \to S^{-1}A/\mathcal{M}S^{-1}A$, where the first map is given by $a \to a/1$ and the second by $a/s \to (a/s) + \mathcal{M}S^{-1}A$.

1. Show that the kernel of the map is $\mathcal{M}$, so by the factor theorem, we have a monomorphism $h : A/\mathcal{M} \to S^{-1}A/\mathcal{M}S^{-1}A$.
2. Let $a/s \in S^{-1}A$. Show that for some $b \in A$ we have $bs \equiv 1 \mod \mathcal{M}$.
3. Show that $(a/s) + \mathcal{M}S^{-1}A = h(ab)$, so h is surjective and therefore an isomorphism.

Consequently, $S^{-1}A/\mathcal{M}S^{-1}A \cong A/\mathcal{M}$, which is the result we need.

4.2 Norms of Ideals

4.2.1 Definitions and Comments

We are familiar with the norm of an element of a field, and we are going to extend the idea to ideals. We assume the $AKLB$ setup with $A = \mathbb{Z}$, so that B is a *number ring*, that is, the ring of algebraic integers of a number field L. If I is a nonzero ideal of B, we define the *norm* of I by $N(I) = |B/I|$. We will show that the norm is finite, so if P is a nonzero prime ideal of B, then B/P is a finite field. Also, N has a multiplicative property analogous to the formula $N(xy) = N(x)N(y)$ for elements. [See (2.1.3), equation (2).]

4.2.2 Proposition

Let b be any nonzero element of the ideal I of B, and let $m = N_{L/\mathbb{Q}}(b) \in \mathbb{Z}$. Then $m \in I$ and $|B/mB| = m^n$, where $n = [L : \mathbb{Q}]$.

Proof. By (2.1.6), $m = bc$ where c is a product of conjugates of b. But a conjugate of an algebraic integer is an algebraic integer. (If a monomorphism is applied to an equation of integral dependence, the result is an equation of integral dependence.) Thus $c \in B$, and since $b \in I$, we have $m \in I$. Now by (2.3.9), B is the direct sum of n copies of $\mathbb{Z}$, hence by the first isomorphism theorem, B/mB is the direct sum of n copies of $\mathbb{Z}/m\mathbb{Z}$. Consequently, $|B/mB| = m^n$. ♣

4.2.3 Corollary

If I is any nonzero ideal of B, then $N(I)$ is finite. In fact, if m is as in (4.2.2), then $N(I)$ divides m^n.

Proof. Observe that $(m) \subseteq I$, hence

$$\frac{B/(m)}{B/I} \cong I/(m). \ \clubsuit$$

4.2.4 Corollary

Every nonzero ideal I of B is a free abelian group of rank n.

Proof. By the simultaneous basis theorem, we may represent B as the direct sum of n copies of $\mathbb{Z}$, and I as the direct sum of $a_1\mathbb{Z}, \ldots, a_r\mathbb{Z}$, where $r \leq n$ and the a_i are positive integers such that a_i divides a_{i+1} for all i. Thus B/I is the direct sum of r cyclic groups (whose orders are $a_1, \ldots, a_r$) and $n - r$ copies of $\mathbb{Z}$. If $r < n$, then at least one copy of $\mathbb{Z}$ appears, and $|B/I|$ cannot be finite. ♣

4.2.5 Computation of the Norm

Suppose that $\{x_1, \ldots, x_n\}$ is a $\mathbb{Z}$-basis for B, and $\{z_1, \ldots, z_n\}$ is a basis for I. Each z_i is a linear combination of the x_i with integer coefficients, in matrix form $z = Cx$. We claim that the norm of I is the absolute value of the determinant of C. To verify this, first look at the special case $x_i = y_i$ and $z_i = a_i y_i$, as in the proof of (4.2.4). Then C is a diagonal

matrix with entries a_i, and the result follows. But the special case implies the general result, because any matrix corresponding to a change of basis of B or I is unimodular, in other words, has integer entries and determinant ± 1. [See (2.3.9) and (2.3.10).]

Now with $z = Cx$ as above, the discriminant of x is the field discriminant d, and the discriminant of z is $D(z) = (\det C)^2 d$ by (2.3.2). We have just seen that $N(I) = |\det C|$, so we have the following formula for computing the norm of an ideal I. If z is a $\mathbb{Z}$-basis for I, then

$$N(I) = \left| \frac{D(z)}{d} \right|^{1/2}.$$

There is a natural relation between the norm of a principal ideal and the norm of the corresponding element.

4.2.6 Proposition

If $I = (a)$ with $a \neq 0$, then $N(I) = |N_{L/\mathbb{Q}}(a)|$.

Proof. If x is a $\mathbb{Z}$-basis for B, then ax is a $\mathbb{Z}$-basis for I. By (2.3.3), $D(ax)$ is the square of the determinant whose ij entry is $\sigma_i(ax_j) = \sigma_i(a)\sigma_i(x_j)$. By (4.2.5), the norm of I is $|\sigma_1(a) \cdots \sigma_n(a)| = |N_{L/\mathbb{Q}}(a)|$. ♣

In the proof of (4.2.6), we cannot invoke (2.3.2) to get $D(ax_1, \ldots, ax_n) = (a^n)^2 D(x_1, \ldots, x_n)$, because we need not have $a \in \mathbb{Q}$.

We now establish the multiplicative property of ideal norms.

4.2.7 Theorem

If I and J are nonzero ideals of B, then $N(IJ) = N(I)N(J)$.

Proof. By unique factorization, we may assume without loss of generality that J is a prime ideal P. By the third isomorphism theorem, $|B/IP| = |B/I|\ |I/IP|$, so we must show that $|I/IP|$ is the norm of P, that is, $|B/P|$. But this has already been done in the first part of the proof of (4.1.6). ♣

4.2.8 Corollary

Let I be a nonzero ideal of B. If $N(I)$ is prime, then I is a prime ideal.

Proof. Suppose I is the product of two ideals I_1 and I_2. By (4.2.7), $N(I) = N(I_1)N(I_2)$, so by hypothesis, $N(I_1) = 1$ or $N(I_2) = 1$. Thus either I_1 or I_2 is the identity element of the ideal group, namely B. Therefore, the prime factorization of I is I itself, in other words, I is a prime ideal. ♣

4.2.9 Proposition

$N(I) \in I$, in other words, I divides $N(I)$. [More precisely, I divides the principal ideal generated by $N(I)$.]

Proof. Let $N(I) = |B/I| = r$. If $x \in B$, then $r(x + I)$ is 0 in B/I, because the order of any element of a group divides the order of the group. Thus $rx \in I$, and in particular we may take $x = 1$ to conclude that $r \in I$. ♣

4.2.10 Corollary

If I is a nonzero prime ideal of B, then I divides (equivalently, contains) exactly one rational prime p.

Proof. By (4.2.9), I divides $N(I) = p_1^{m_1} \cdots p_t^{m_t}$, so I divides some p_i. But if I divides two distinct primes p and q, then there exist integers u and v such that $up + vq = 1$. Thus I divides 1, so $I = B$, a contradiction. Therefore I divides exactly one p. ♣

4.2.11 The Norm of a Prime Ideal

If we can compute the norm of every nonzero prime ideal P, then by multiplicativity, we can calculate the norm of any nonzero ideal. Let p be the unique rational prime in P, and recall from (4.1.3) that the relative degree of P over p is $f(P) = [B/P : \mathbb{Z}/p\mathbb{Z}]$. Therefore

$$N(P) = |B/P| = p^{f(P)}.$$

Note that by (4.2.6), the norm of the principal ideal (p) is $|N(p)| = p^n$, so $N(P) = p^m$ for some $m \leq n$. This conclusion also follows from the above formula $N(P) = p^{f(P)}$ and the ram-rel identity (4.1.6).

Here are two other useful finiteness results.

4.2.12 Proposition

A rational integer m can belong to only finitely many ideals of B.

Proof. We have $m \in I$ iff I divides (m), and by unique factorization, (m) has only finitely many divisors. ♣

4.2.13 Corollary

Only finitely many ideals can have a given norm.

Proof. If $N(I) = m$, then by (4.2.9), $m \in I$, and the result follows from (4.2.12). ♣

Problems For Section 4.2

This problem set will give the proof that a rational prime p ramifies in the number field L if and only if p divides the field discriminant $d = d_{L/\mathbb{Q}}$.

1. Let $(p) = pB$ have prime factorization $\prod_i P_i^{e_i}$. Show that p ramifies if and only if the ring $B/(p)$ has nonzero nilpotent elements.

Now as in (2.1.1), represent elements of B by matrices with respect to an integral basis $\omega_1, \ldots, \omega_n$ of B. Reduction of the entries mod p gives matrices representing elements of $B/(p)$.

2. Show that a nilpotent element (or matrix) has zero trace.

Suppose that $A(\beta)$, the matrix representing the element β, is nilpotent mod p. Then $A(\beta\omega_i)$ will be nilpotent mod p for all i, because $\beta\omega_i$ is nilpotent mod p.
3. By expressing β in terms of the ω_i and computing the trace of $A(\beta\omega_j)$, show that if β is nilpotent mod p and $\beta \notin (p)$, then $d \equiv 0 \mod p$, hence p divides d.

Now assume that p does not ramify.
4. Show that $B/(p)$ is isomorphic to a finite product of finite fields F_i of characteristic p.

Let $\pi_i : B \to B/(p) \to F_i$ be the composition of the canonical map from B onto $B/(p)$ and the projection from $B/(p)$ onto F_i.
5. Show that the trace form $T_i(x, y) = T_{F_i/\mathbb{F}_p}(\pi_i(x)\pi_i(y))$ is nondegenerate, and conclude that $\sum_i T_i$ is also nondegenerate.

We have $d = \det T(\omega_i\omega_j)$, in other words, the determinant of the matrix of the bilinear form $T(x, y)$ on B, with respect to the basis $\{\omega_1, \ldots, \omega_n\}$. Reducing the matrix entries mod p, we get the matrix of the reduced bilinear form T_0 on the $\mathbb{F}_p$-vector space $B/(p)$.
6. Show that T_0 coincides with $\sum_i T_i$, hence T_0 is nondegenerate. Therefore $d \not\equiv 0 \mod p$, so p does not divide d.

As a corollary, it follows that only finitely many primes can ramify in L.

4.3 A Practical Factorization Theorem

The following result, usually credited to Kummer but sometimes attributed to Dedekind, allows, under certain conditions, an efficient factorization of a rational prime in a number field.

4.3.1 Theorem

Let L be a number field of degree n over $\mathbb{Q}$, and assume that the ring B of algebraic integers of L is $\mathbb{Z}[\theta]$ for some $\theta \in B$. Thus $1, \theta, \theta^2, \ldots, \theta^{n-1}$ form an integral basis of B. Let p be a rational prime, and let f be the minimal polynomial of θ over $\mathbb{Q}$. Reduce the coefficients of f modulo p to obtain $\overline{f} \in \mathbb{Z}[X]$. Suppose that the factorization of $\overline{f}$ into irreducible polynomials over $\mathbb{F}_p$ is given by

$$\overline{f} = h_1^{e_1} \cdots h_r^{e_r}.$$

Let f_i be any polynomial in $\mathbb{Z}[X]$ whose reduction mod p is h_i. Then the ideal

$$P_i = (p, f_i(\theta))$$

is prime, and the prime factorization of (p) in B is

$$(p) = P_1^{e_1} \cdots P_r^{e_r}.$$

Proof. Adjoin a root θ_i of h_i to produce the field $\mathbb{F}_p[\theta_i] \cong \mathbb{F}_p[X]/h_i(X)$. The assignment $\theta \to \theta_i$ extends by linearity (and reduction of coefficients mod p) to an epimorphism $\lambda_i : \mathbb{Z}[\theta] \to \mathbb{F}_p[\theta_i]$. Since $\mathbb{F}_p[\theta_i]$ is a field, the kernel of λ_i is a maximal, hence prime, ideal of $\mathbb{Z}[\theta] = B$. Since λ_i maps $f_i(\theta)$ to $h_i(\theta_i) = 0$ and also maps p to 0, it follows that $P_i \subseteq \ker \lambda_i$. We claim that $P_i = \ker \lambda_i$. To prove this, assume $g(\theta) \in \ker \lambda_i$. With a

subscript 0 indicating reduction of coefficients mod p, we have $g_0(\theta_i) = 0$, hence h_i, the minimal polynomial of θ_i, divides g_0. If $g_0 = q_0 h_i$, then $g - q f_i \equiv 0 \mod p$. Therefore

$$g(\theta) = [g(\theta) - q(\theta) f_i(\theta)] + q(\theta) f_i(\theta)$$

so $g(\theta)$ is the sum of an element of (p) and an element of $(f_i(\theta))$. Thus $\ker \lambda_i \subseteq P_i$, so $P_i = \ker \lambda_i$, a prime ideal.

We now show that (p) divides $P_1^{e_1} \cdots P_r^{e_r}$. We use the identity $(I+I_1)(I+I_2) \subseteq I+I_1 I_2$, where I, I_1 and I_2 are ideals. We begin with $P_1 = (p) + (f_1(\theta))$, and compute

$$P_1^2 \subseteq (p) + (f_1(\theta))^2, \ldots, P_1^{e_1} \cdots P_r^{e_r} \subseteq (p) + (f_1(\theta))^{e_1} \cdots (f_r(\theta))^{e_r}.$$

But the product of the $f_i(\theta)^{e_i}$ coincides mod p with $\prod_{i=1}^r h_i(\theta) = \overline{f}(\theta) = 0$. We conclude that $\prod_{i=1}^r P_i^{e_i} \subseteq (p)$, as asserted.

We now know that $(p) = P_1^{k_1} \cdots P_r^{k_r}$ with $0 \leq k_i \leq e_i$. (Actually, $k_i > 0$ since $p \in \ker \lambda_i = P_i$, so P_i divides (p). But we will not need this refinement.) By hypothesis, $B/P_i = \mathbb{Z}[\theta]/P_i$, which is isomorphic to $\mathbb{F}_p[\theta_i]$, as observed at the beginning of the proof. Thus the norm of P_i is $|\mathbb{F}_p[\theta_i]| = p^{d_i}$, where d_i is the degree of h_i. By (4.2.6), (4.2.7) and equation (3) of (2.1.3),

$$p^n = N((p)) = \prod_{i=1}^r N(P_i)^{k_i} = \prod_{i=1}^r p^{d_i k_i}$$

hence $n = d_1 k_1 + \cdots + d_r k_r$. But n is the degree of the monic polynomial f, which is the same as $\deg \overline{f} = d_1 e_1 + \cdots + d_r e_r$. Since $k_i \leq e_i$ for every i, we have $k_i = e_i$ for all i, and the result follows. ♣

4.3.2 Prime Factorization in Quadratic Fields

We consider $L = \mathbb{Q}(\sqrt{m})$, where m is a square-free integer, and factor the ideal (p) in the ring B of algebraic integers of L. By the ram-rel identity (4.1.6), there will be three cases:

(1) $g = 2, e_1 = e_2 = f_1 = f_2 = 1$. Then (p) is the product of two distinct prime ideals P_1 and P_2, and we say that p *splits* in L.

(2) $g = 1, e_1 = 1, f_1 = 2$. Then (p) is a prime ideal of B, and we say that p *remains prime* in L or that p is *inert*.

(3) $g = 1, e_1 = 2, f_1 = 1$. Then $(p) = P_1^2$ for some prime ideal P_1, and we say that p *ramifies* in L.

We will examine all possibilities systematically.

(a) Assume p is an odd prime not dividing m. Then p does not divide the discriminant, so p does not ramify.

(a1) If m is a quadratic residue mod p, then p splits. Say $m \equiv n^2 \mod p$. Then $x^2 - m$ factors mod p as $(x+n)(x-n)$, so $(p) = (p, n+\sqrt{m})\ (p, n-\sqrt{m})$.

(a2) If m is not a quadratic residue mod p, then $x^2 - m$ cannot be the product of two linear factors, hence $x^2 - m$ is irreducible mod p and p remains prime.

(b) Let p be any prime dividing m. Then p divides the discriminant, hence p ramifies. Since $x^2 - m \equiv x^2 = xx \mod p$, we have $(p) = (p, \sqrt{m})^2$.

This takes care of all odd primes, and also $p = 2$ with m even.

(c) Assume $p = 2$, m odd.

(c1) Let $m \equiv 3 \mod 4$. Then 2 divides the discriminant $D = 4m$, so 2 ramifies. We have $x^2 - m \equiv (x+1)^2 \mod 2$, so $(2) = (2, 1 + \sqrt{m})^2$.

(c2) Let $m \equiv 1 \mod 8$, hence $m \equiv 1 \mod 4$. An integral basis is $\{1, (1+\sqrt{m})/2\}$, and the discriminant is $D = m$. Thus 2 does not divide D, so 2 does not ramify. We claim that $(2) = (2, (1+\sqrt{m})/2)\ (2, (1-\sqrt{m})/2)$. To verify this note that the right side is $(2, 1-\sqrt{m}, 1+\sqrt{m}, (1-m)/4)$. This coincides with (2) because $(1-m)/4$ is an even integer and $1 - \sqrt{m} + 1 + \sqrt{m} = 2$.

If $m \equiv 3$ or $7 \bmod 8$, then $m \equiv 3 \mod 4$, so there is only one remaining case.

(c3) Let $m \equiv 5 \mod 8$, hence $m \equiv 1 \mod 4$, so $D = m$ and 2 does not ramify. Consider $f(x) = x^2 - x + (1-m)/4$ over B/P, where P is any prime ideal lying over (2). The roots of f are $(1 \pm \sqrt{m})/2$, so f has a root in B, hence in B/P. But there is no root in $\mathbb{F}_2$, because $(1-m)/4 \equiv 1 \mod 2$. Thus B/P and $\mathbb{F}_2$ cannot be isomorphic. If (2) factors as $Q_1 Q_2$, then the norm of (2) is 4, so Q_1 and Q_2 have norm 2, so the B/Q_i are isomorphic to $\mathbb{F}_2$, which contradicts the argument just given. Therefore 2 remains prime.

You probably noticed something suspicious in cases (a) and (b). In order to apply (4.3.1), 1 and $\sqrt{m}$ must form an integral basis, so $m \not\equiv 1 \mod 4$, as in (2.3.11). But we can repair the damage. In (a1), verify directly that the factorization of (p) is as given. The key point is that the ideal $(p, n+\sqrt{m})\ (p, n-\sqrt{m})$ contains $p(n+\sqrt{m}+n-\sqrt{m}) = 2np$, and if p divides n, then p divides $(m-n^2) + n^2 = m$, contradicting the assumption of case (a). Thus the greatest common divisor of p^2 and $2np$ is p, so p belongs to the ideal. Since every generator of the ideal is a multiple of p, the result follows. In (a2), suppose $(p) = Q_1 Q_2$. Since the norm of p is p^2, each Q_i has norm p, so B/Q_i must be isomorphic to $\mathbb{F}_p$. But $\sqrt{m} \in B$, so m has a square root in B/Q_i [see (4.1.4)]. But case (a2) assumes that there is no square root of m in $\mathbb{F}_p$, a contradiction. Finally, case (b) is similar to case (a1). We have $p|m$, but p^2 does not divide the square-free integer m, so the greatest common divisor of p^2 and m is p.

Problems For Section 4.3

1. In the exercises for Section 3.4, we factored (2) and (3) in the ring B of algebraic integers of $L = \mathbb{Q}(\sqrt{-5})$, using ad hoc techniques. Using the results of this section, derive the results rigorously.

2. Continuing Problem 1, factor (5), (7) and (11).

3. Let $L = \mathbb{Q}(\sqrt[3]{2})$, and assume as known that the ring of algebraic integers is $B = \mathbb{Z}[\sqrt[3]{2}]$. Find the prime factorization of (5).