# Chapter 8

# Factoring of Prime Ideals in Galois Extensions

## 8.1 Decomposition and Inertia Groups

We return to the general AKLB setup: $A$ is a Dedekind domain with fraction field $K$, $L$ is a finite separable extension of $K$, and $B$ is the integral closure of $A$ in $L$. But now we add the condition that the extension $L/K$ is normal, hence Galois. We will see shortly that the Galois assumption imposes a severe constraint on the numbers $e_i$ and $f_i$ in the ram-rel identity (4.1.6). Throughout this chapter, $G$ will denote the Galois group $\mathrm{Gal}(L/K)$.

### 8.1.1 Proposition

If $\sigma \in G$, then $\sigma(B) = B$. If $Q$ is a prime ideal of $B$, then so is $\sigma(Q)$. Moreover, if $Q$ lies above the nonzero prime ideal $P$ of $A$, then so does $\sigma(Q)$. Thus $G$ acts on the set of prime ideals lying above $P$.

*Proof.* If $x \in B$, then $\sigma(x) \in B$ (apply $\sigma$ to an equation of integral dependence). Thus $\sigma(B) \subseteq B$. But $\sigma^{-1}(B)$ is also contained in $B$, hence $B = \sigma\sigma^{-1}(B) \subseteq \sigma(B)$. If $PB = \prod Q_i^{e_i}$, then apply $\sigma$ to get $PB = \prod \sigma(Q_i)^{e_i}$. The $\sigma(Q_i)$ must be prime ideals because $\sigma$ preserves all algebraic relations. Note also that $\sigma$ is a $K$-automorphism, hence fixes every element of $A$ (and of $P$). Therefore $Q \cap A = P \Rightarrow \sigma(Q) \cap A = P$. ♣

We now show that the action of $G$ is transitive.

### 8.1.2 Theorem

Let $Q$ and $Q_1$ be prime ideals lying above $P$. Then for some $\sigma \in G$ we have $\sigma(Q) = Q_1$.

*Proof.* If the assertion is false, then for each $\sigma$, the ideals $Q_1$ and $\sigma(Q)$ are maximal and distinct, so $Q_1 \not\subseteq \sigma(Q)$. By the prime avoidance lemma (Section 3.1, exercises), there is an element $x \in Q_1$ belonging to none of the $\sigma(Q)$. Computing the norm of $x$ relative to $L/K$, we have $N(x) = \prod_{\sigma \in G} \sigma(x)$ by (2.1.6). But one of the $\sigma$'s is the identity, $Q_1$ is an ideal, and [by (8.1.1)] $\sigma(x) \in B$ for all $\sigma$. Consequently, $N(x) \in Q_1$. But $N(x) \in A$ by

(2.2.2), so $N(x) \in Q_1 \cap A = P = Q \cap A$. Thus $N(x)$ belongs to the prime ideal $Q$, and therefore some $\sigma^{-1}(x)$ belongs to $Q$ as well. This gives $x \in \sigma(Q)$, a contradiction. ♣

### 8.1.3 Corollary

In the factorization $PB = \prod_{i=1}^{g} P_i^{e_i}$ of the nonzero prime ideal $P$, the ramification indices $e_i$ are the same for all $i$, as are the relative degrees $f_i$. Thus the ram-rel identity simplifies to $efg = n$, where $n = [L : K] = |G|$.

*Proof.* This follows from (8.1.2), along with the observation that an automorphism $\sigma$ preserves all algebraic relations. ♣

Since we have a group $G$ acting on the prime factors of $PB$, it is natural to consider the stabilizer subgroup of each prime factor $Q$.

### 8.1.4 Definitions and Comments

We say that the prime ideals $\sigma(Q), \sigma \in G$, are the *conjugates* of $Q$. Thus (8.1.2) says that all prime factors of $PB$ are conjugate. The *decomposition group* of $Q$ is the subgroup $D$ of $G$ consisting of those $\sigma \in G$ such that $\sigma(Q) = Q$. (This does *not* mean that $\sigma$ fixes every element of $Q$.) By the orbit-stabilizer theorem, the size of the orbit of $Q$ is the index of the stabilizer subgroup $D$. Since there is only one orbit, of size $g$,

$$g = [G : D] = |G|/|D|, \text{ hence } |D| = n/g = efg/g = ef,$$

independent of $Q$. Note also that distinct conjugates of $Q$ determine distinct cosets of $D$. For if $\sigma_1 D = \sigma_2 D$, then $\sigma_2^{-1}\sigma_1 \in D$, so $\sigma_1(Q) = \sigma_2(Q)$.

There is a particular subgroup of $D$ that will be of interest. By (8.1.1), $\sigma(B) = B$ for every $\sigma \in G$. If $\sigma \in D$, then $\sigma(Q) = Q$. It follows that $\sigma$ induces an automorphism $\overline{\sigma}$ of $B/Q$. (Note that $x \equiv y \mod Q$ iff $\sigma x \equiv \sigma y \mod Q$.) Since $\sigma$ is a $K$-automorphism, $\overline{\sigma}$ is an $A/P$-automorphism. The mapping $\sigma \to \overline{\sigma}$ is a group homomorphism from $D$ to the group of $A/P$-automorphisms of $B/Q$.

### 8.1.5 Definition

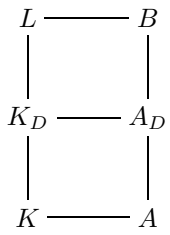
The kernel $I$ of the above homomorphism, that is, the set of all $\sigma \in D$ such that $\overline{\sigma}$ is trivial, is called the *inertia group* of $Q$.

### 8.1.6 Remarks

The inertia group is a normal subgroup of the decomposition group, as it is the kernel of a homomorphism. It is given explicitly by

$$I = \{\sigma \in D : \sigma(x) + Q = x + Q \ \forall x \in B\} = \{\sigma \in D : \sigma(x) - x \in Q \ \forall x \in B\}.$$

We now introduce an intermediate field and ring into the basic $AKLB$ setup, as follows.




Take $K_D$ to be the fixed field of $D$, and let $A_D = B \cap K_D$ be the integral closure of $A$ in $K_D$. Let $P_D$ be the prime ideal $Q \cap A_D$. Note that $Q$ is the only prime factor of $P_D B$. This is because all primes in the factorization are conjugate, and $\sigma(Q) = Q$ for all $\sigma \in D$, by definition of $D$.

### 8.1.7 Lemma

Let $P_D B = Q^{e'}$ and $f' = [B/Q : A_D/P_D]$. Then $e' = e$ and $f' = f$. Moreover, $A/P \cong A_D/P_D$.

*Proof.* First, observe that by the ram-rel identity [see (8.1.3)], $e'f' = [L : K_D]$, which is $|D|$ by the fundamental theorem of Galois theory. But $|D| = ef$ by (8.1.4), so $e'f' = ef$. Now as in (4.1.3)-(4.1.5), $A/P \subseteq A_D/P_D \subseteq B/Q$, so $f' \leq f$. Also, $PA_D \subseteq P_D$, so $P_D$ divides $PA_D$, hence $P_D B$ divides $PA_D B = PB$. Consequently, $e' \leq e$, and this forces $e' = e$ and $f' = f$. Thus the dimension of $B/Q$ over $A_D/P_D$ is the same as the dimension of $B/Q$ over $A/P$. Since $A/P$ can be regarded as a subfield of $A_D/P_D$, the proof is complete. ♣

### 8.1.8 Theorem

Assume $(B/Q)/(A/P)$ separable. The homomorphism $\sigma \to \overline{\sigma}$ of $D$ to $\mathrm{Gal}[(B/Q)/(A/P)]$ introduced in (8.1.4) is surjective with kernel $I$. Therefore $\mathrm{Gal}[(B/Q)/(A/P)] \cong D/I$.

*Proof.* Let $\overline{x}$ be a primitive element of $B/Q$ over $A/P$. Let $x \in B$ be a representative of $\overline{x}$. Let $h(X) = X^r + a_{r-1}X^{r-1} + \cdot + a_0$ be the minimal polynomial of $x$ over $K_D$; the coefficients $a_i$ belong to $A_D$ by (2.2.2). The roots of $h$ are all of the form $\sigma(x), \sigma \in D$. (We are working in the extension $L/K_D$, with Galois group $D$.) By (8.1.7), if we reduce the coefficients of $h$ mod $P_D$, the resulting polynomial $\overline{h}(X)$ has coefficients in $A/P$. The roots of $\overline{h}$ are of the form $\overline{\sigma}(\overline{x}), \sigma \in D$ (because $\overline{x}$ is a primitive element). Since $\sigma \in D$ means that $\sigma(Q) = Q$, all conjugates of $\overline{x}$ over $A/P$ lie in $B/Q$. By the basic theory of splitting fields, $B/Q$ is a Galois extension of $A/P$.

To summarize, since every conjugate of $\overline{x}$ over $A/P$ is of the form $\overline{\sigma}(\overline{x})$, every $A/P$-automorphism of $B/Q$ (necessarily determined by its action on $\overline{x}$), is of the form $\overline{\sigma}$ where $\sigma \in D$. Since $\overline{\sigma}$ is trivial iff $\sigma \in I$, it follows that the map $\sigma \to \overline{\sigma}$ is surjective and has kernel $I$. ♣

### 8.1.9 Corollary

The order of $I$ is $e$. Thus the prime ideal $P$ does not ramify if and only if the inertia group of every prime ideal $Q$ lying over $P$ is trivial.

*Proof.* By definition of relative degree, the order of $\mathrm{Gal}[(B/Q)/(A/P)]$ is $f$. By (8.1.4), the order of $D$ is $ef$. Thus by (8.1.8), the order of $I$ must be $e$. ♣

### Problems For Section 8.1

1. Let $D(Q)$ be the decomposition group of the prime ideal $Q$. It follows from the definition of stabilizer subgroup that $D(\sigma(Q)) = \sigma D(Q)\sigma^{-1}$ for every $\sigma \in G$. Show that the inertia subgroup also behaves in this manner, that is, $I(\sigma(Q)) = \sigma I(Q)\sigma^{-1}$.
2. If $L/K$ is an abelian extension (the Galois group $G = \mathrm{Gal}(L/K)$ is abelian), show that the groups $D(\sigma(Q)), \sigma \in G$, are all equal, as are the $I(\sigma(Q)), \sigma \in G$. Show also that the groups depend only on the prime ideal $P$ of $A$.

## 8.2 The Frobenius Automorphism

In the basic $AKLB$ setup, with $L/K$ a Galois extension, we now assume that $K$ and $L$ are number fields.

### 8.2.1 Definitions and Comments

Let $P$ be a prime ideal of $A$ that does not ramify in $B$, and let $Q$ be a prime lying over $P$. By (8.1.9), the inertia group $I(Q)$ is trivial, so by (8.1.8), $\mathrm{Gal}[(B/Q)/(A/P)]$ is isomorphic to the decomposition group $D(Q)$. But $B/Q$ is a finite extension of the finite field $A/P$ [see (4.1.3)], so the Galois group is cyclic. Moreover, there is a canonical generator given by $x+Q \to x^q+Q, x \in B$, where $q = |A/P|$. Thus we have identified a distinguished element $\sigma \in D(Q)$, called the *Frobenius automorphism*, or simply the *Frobenius*, of $Q$, relative to the extension $L/K$. The Frobenius automorphism is determined by the requirement that for every $x \in B$,

$$\sigma(x) \equiv x^q \mod Q.$$

We use the notation $\left[\frac{L/K}{Q}\right]$ for the Frobenius automorphism. The behavior of the Frobenius under conjugation is similar to the behavior of the decomposition group as a whole (see the exercises in Section 8.1).

### 8.2.2 Proposition

If $\tau \in G$, then $\left[\frac{L/K}{\tau(Q)}\right] = \tau \left[\frac{L/K}{Q}\right] \tau^{-1}$.

*Proof.* If $x \in B$, then $\left[\frac{L/K}{Q}\right] \tau^{-1}x \equiv (\tau^{-1}x)^q = \tau^{-1}x^q \mod Q$. Apply $\tau$ to both sides to conclude that $\tau \left[\frac{L/K}{Q}\right] \tau^{-1}$ satisfies the defining equation for $\left[\frac{L/K}{\tau(Q)}\right]$. Since the Frobenius is determined by its defining equation, the result follows. ♣

### 8.2.3 Corollary

If $L/K$ is abelian, then $\left[\frac{L/K}{Q}\right]$ depends only on $P$, and we write the Frobenius automorphism as $\left(\frac{L/K}{P}\right)$, and sometimes call it the *Artin symbol*.

*Proof.* By (8.2.2), the Frobenius is the same for all conjugate ideals $\tau(Q), \tau \in G$, hence by (8.1.2), for all prime ideals lying over $P$. ♣

### 8.2.4 Intermediate Fields

We now introduce an intermediate field between $K$ and $L$, call it $F$. We can then lift $P$ to the ring of algebraic integers in $F$, namely $B \cap F$. A prime ideal lying over $P$ has the form $Q \cap F$, where $Q$ is a prime ideal of $PB$. We will compare decomposition groups with respect to the fields $L$ and $F$, with the aid of the identity

$$[B/Q : A/P] = [B/Q : (B \cap F)/(Q \cap F)][(B \cap F)/(Q \cap F) : A/P].$$

The term on the left is the order of the decomposition group of $Q$ over $P$, denoted by $D(Q, P)$. (We are assuming that $P$ does not ramify, so $e = 1$.) The first term on the right is the order of the decomposition group of $Q$ over $Q \cap F$. The second term on the right is the relative degree of $Q \cap F$ over $P$, call it $f$. Thus

$$|D(Q, Q \cap F)| = |D(Q, P)|/f$$

Since $D = D(Q, P)$ is cyclic and is generated by the Frobenius automorphism $\sigma$, the unique subgroup of $D$ with order $|D|/f$ is generated by $\sigma^f$. Note that $D(Q, Q \cap F)$ is a subgroup of $D(Q, P)$, because $\mathrm{Gal}(L/F)$ is a subgroup of $\mathrm{Gal}(L/K)$. It is natural to expect that the Frobenius automorphism of $Q$, relative to the extension $L/F$, is $\sigma^f$.

### 8.2.5 Proposition

$\left[\frac{L/F}{Q}\right] = \left[\frac{L/K}{Q}\right]^f$.

*Proof.* Let $\sigma = \left[\frac{L/K}{Q}\right]$. Then $\sigma \in D$, so $\sigma(Q) = Q$; also $\sigma(x) \equiv x^q \mod Q, x \in B$, where $q = |A/P|$. Thus $\sigma^f(Q) = Q$ and $\sigma^f(x) \equiv x^{q^f}$. Since $q^f$ is the cardinality of the field $(B \cap F)/(Q \cap F)$, the result follows. ♣

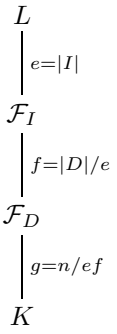
### 8.2.6 Proposition

If the extension $F/K$ is Galois, then the restriction of $\sigma = \left[\frac{L/K}{Q}\right]$ to $F$ is $\left[\frac{F/K}{Q \cap F}\right]$.

*Proof.* Let $\sigma_1$ be the restriction of $\sigma$ to $F$. Since $\sigma(Q) = Q$, it follows that $\sigma_1(Q \cap F) = Q \cap F$. (Note that $F/K$ is normal, so $\sigma_1$ is an automorphism of $F$.) Thus $\sigma_1$ belongs to $D(Q \cap F, P)$. Since $\sigma(x) \equiv x^q \mod Q$, we have $\sigma_1(x) \equiv x^q \mod (Q \cap F)$, where $q = |A/P|$. Consequently, $\sigma_1 = \left[\frac{F/K}{Q \cap F}\right]$. ♣

### 8.2.7 Definitions and Comments

We may view the lifting from the base field $K$ to the extension field $L$ as occurring in three distinct steps. Let $\mathcal{F}_D$ be the *decomposition field* of the extension, that is, the fixed field of the decomposition group $D$, and let $\mathcal{F}_I$ be the *inertia field*, the fixed field of the inertia group $I$. We have the following diagram:




All ramification takes place at the top (call it level 3), and all splitting at the bottom (level 1). There is inertia in the middle (level 2). Alternatively, the results can be expressed in tabular form:

| | e | f | g |
|---|---|---|---|
| Level 1 | 1 | 1 | g |
| 2 | 1 | f | 1 |
| 3 | e | 1 | 1 |

As we move up the diagram, we multiply the ramification indices and relative degrees. This is often expressed by saying that $e$ and $f$ are *multiplicative in towers*. The basic point is that if $Q = Q_1^{e_1} \cdots$ and $Q_1 = Q_2^{e_2} \cdots$, then $Q = Q_2^{e_1 e_2} \cdots$. The multiplicativity of $f$ follows because $f$ is a vector space dimension.

## 8.3 Applications

### 8.3.1 Cyclotomic Fields

Let $\zeta$ be a primitive $m^{\text{th}}$ root of unity, and let $L = \mathbb{Q}(\zeta)$ be the corresponding cyclotomic field. (We are in the $AKLB$ setup with $A = \mathbb{Z}$ and $K = \mathbb{Q}$.) Assume that $p$ is a rational prime that does not divide $m$. Then by (7.2.5) and the exercises for Section 4.2, $p$ is unramified. Thus $(p)$ factors in $B$ as $Q_1 \cdots Q_g$, where the $Q_i$ are distinct prime ideals. Moreover, the relative degree $f$ is the same for all $Q_i$, because the extension $L/\mathbb{Q}$ is Galois. In order to say more about $f$, we find the Frobenius automorphism $\sigma$ explicitly. The defining equation is $\sigma(x) \equiv x^p \mod Q_i$ for all $i$, and consequently

$$\sigma(\zeta) = \zeta^p.$$

(The idea is that the roots of unity remain distinct when reduced mod $Q_i$, because the polynomial $X^n - 1$ is separable over $\mathbb{F}_p$.)

Now the order of $\sigma$ is the size of the decomposition group $D$, which is $f$. Thus $f$ is the smallest positive integer such that $\sigma^f(\zeta) = \zeta$. Since $\zeta$ is a primitive $m^{\text{th}}$ root of unity, we conclude that

$$f \text{ is the smallest positive integer such that } p^f \equiv 1 \mod m.$$

Once we know $f$, we can find the number of prime factors $g = n/f$, where $n = \varphi(m)$. (We already know that $e = 1$ because $p$ is unramified.)

When $p$ divides $m$, the analysis is more complicated, and we will only state the result. Say $m = p^a m_1$, where $p$ does not divide $m_1$. Then $f$ is the smallest positive integer such that $p^f \equiv 1 \mod m_1$. The factorization is $(p) = (Q_1 \cdots Q_g)^e$, with $e = \varphi(p^a)$. The $Q_i$ are distinct prime ideals, each with relative degree $f$. The number of distinct prime factors is $g = \varphi(m_1)/f$.

We will now give a proof of Gauss' law of quadratic reciprocity.

### 8.3.2 Proposition

Let $q$ be an odd prime, and let $L = \mathbb{Q}(\zeta_q)$ be the cyclotomic field generated by a primitive $q^{\text{th}}$ root of unity. Then $L$ has a unique quadratic subfield $F$. Explicitly, if $q \equiv 1 \mod 4$, then the quadratic subfield is $\mathbb{Q}(\sqrt{q})$, and if $q \equiv 3 \mod 4$, it is $\mathbb{Q}(\sqrt{-q})$. More compactly, $F = \mathbb{Q}(\sqrt{q^*})$, where $q^* = (-1)^{q-1)/2}q$.

*Proof.* The Galois group of the extension is cyclic of even order $q-1$, hence has a unique subgroup of index 2. Therefore $L$ has a unique quadratic subfield. By (7.1.7) and the exercises to Section 7.1, the field discriminant is $d = (-1)^{(q-1)/2}q^{q-2} \in \mathbb{Q}$. But $\sqrt{d} \notin \mathbb{Q}$, because $d$ has an odd number of factors of $q$. If $q \equiv 1 \mod 4$, then the sign of $d$ is positive and $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{q})$. Similarly, if $q \equiv 3 \mod 4$, then the sign of $d$ is negative and $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{-q})$. [Note that the roots of the cyclotomic polynomial belong to $L$, hence so does $\sqrt{d}$; see (2.3.5).] ♣

### 8.3.3 Remarks

Let $\sigma_p$ be the Frobenius automorphism $\left(\frac{F/\mathbb{Q}}{p}\right)$, where $F$ is the unique quadratic subfield of $L$, and $p$ is an odd prime unequal to $q$. By (4.3.2), case (a1), if $q^*$ is a quadratic residue mod $p$, then $p$ splits, so $g = 2$ and therefore $f = 1$. Thus the decomposition group $D$ is trivial, and since $\sigma_p$ generates $D$, $\sigma_p$ is the identity. If $q^*$ is not a quadratic residue mod $p$, then by (4.3.2), case (a2), $p$ is inert, so $g = 1$, $f = 2$, and $\sigma_p$ is nontrivial. Since the Galois group of $F/\mathbb{Q}$ has only two elements, it may be identified with $\{1, -1\}$ under multiplication, and we may write (using the standard Legendre symbol) $\sigma_p = (\frac{q^*}{p})$. On the other hand, $\sigma_p$ is the restriction of $\sigma = \left(\frac{L/\mathbb{Q}}{p}\right)$ to $F$, by (8.2.6). Thus $\sigma_p$ is the identity on $F$ iff $\sigma$ belongs to $H$, the unique subgroup of $\text{Gal}(L/\mathbb{Q})$ of index 2. This will happen iff $\sigma$ is a square. Now the Frobenius may be viewed as a lifting of the map $x \to x^p \mod q$. [As in (8.3.1), $\sigma(\zeta_q) = \zeta_q^p$.] Thus $\sigma$ will belong to $H$ iff $p$ is a quadratic residue mod $q$. In other words, $\sigma_p = (\frac{p}{q})$.

### 8.3.4 Quadratic Reciprocity

If $p$ and $q$ are distinct odd primes, then

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right).$$

*Proof.* By (8.3.3),

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right) = \left(\frac{(-1)^{(q-1)/2}}{p}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)^{(q-1)/2}\left(\frac{q}{p}\right).$$

But by elementary number theory, or by the discussion in the introduction to Chapter 1,

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2},$$

and the result follows. ♣

### 8.3.5 Remark

Let $L = \mathbb{Q}(\zeta)$, where $\zeta$ is a primitive $p^{th}$ root of unity, $p$ prime. As usual, $B$ is the ring of algebraic integers of $L$. In this case, we can factor $(p)$ in $B$ explicitly. By (7.1.3) and (7.1.5),

$$(p) = (1-\zeta)^{p-1}.$$

Thus the ramification index $e = p-1$ coincides with the degree of the extension. We say that $p$ is *totally ramified*.