7 Galois extensions, Frobenius elements, and the Artin map

In our standard $AKLB$ setup, A is a Dedekind domain, L/K is a finite separable extension of its fraction field, and B is the integral closure of A in L, also a Dedekind domain. We now add the additional hypothesis that the extension L/K is normal, hence Galois, and let $G := \operatorname{Gal}(L/K)$ to denote the Galois group; we will use $AKLBG$ to denote this setup.

7.1 Splitting primes in Galois extensions

We begin by showing that the Galois group G acts on the ideal group of B.

Theorem 7.1. *Assume $AKLBG$ and for each fractional ideal I if B, let*

$$\sigma(I) \coloneqq \{\sigma(x) : x \in I\}.$$

The set $\sigma(I)$ is a fractional ideal of B, and this defines a left G-action on $\mathcal{I}_B$ that commutes with the group operation and restricts to a group action on prime ideals.

Proof. Consider any $\sigma \in G$. We first show that $\sigma(B) = B$. Each $b \in B$ is integral over A, hence $f(b) = 0$ for some monic polynomial $f \in A[x]$. We have

$$0 = \sigma(0) = \sigma(f(b)) = f(\sigma(b)),$$

thus $\sigma(b)$ is also integral over A, hence an element of B, since B is the integral closure of A in L. This proves $\sigma(B) \subseteq B$, and by the same argument $\sigma^{-1}(B) \subseteq B$, and $B \subseteq \sigma(B)$.

We now show that if I is a B-ideal, then so is $\sigma(I)$. We have $\sigma(I) \subseteq \sigma(B) = B$, and $\sigma(I)$ is closed under addition (since I is and σ is an automorphism). If $a \in I$ and $b \in B$ then $\sigma^{-1}(b) \in B$ and $\sigma^{-1}(b)a \in I$, thus $\sigma(\sigma^{-1}(b)a) = b\sigma(a) \in \sigma(I)$. It follows that $\sigma(I)$ is also closed under scalar multiplication by B, hence a B-ideal of B.

W have $\sigma(I) = (0)$ if and only if $I = (0)$, since $\sigma(a) = 0$ if and only if $a = 0$. Each nonzero fractional ideal J has the form $J = xI$, with $x \in L^\times$ and I a nonzero B-ideal, so $\sigma(xI) = \sigma(x)\sigma(I)$ is also a nonzero fractional ideal of B, since $\sigma(x) \in L^\times$ and $\sigma(I)$ is a nonzero B-ideal. Each $\sigma \in G$ thus defines a map $\mathcal{I}_B \to \mathcal{I}_B$, and for any $\sigma, \tau \in G$ and $I \in \mathcal{I}_B$,

$$(\sigma\tau)(I) = \{(\sigma\tau)(x) : x \in I\} = \{\sigma(\tau(x)) : x \in I\} = \{\sigma(y) : y \in \tau(I)\} = \sigma(\tau(I)),$$

so G acts on the set $\mathcal{I}_B$ (with the action on the left).

Now let $I, J \in \mathcal{I}_B$ and $\sigma \in G$. Each $x \in IJ$ has the form $x = a_1b_1 + \cdots + a_nb_n$ with $a_i \in I$ and $b_i \in J$, and $\sigma(x) = \sigma(a_1)\sigma(b_1) + \cdots + \sigma(a_n)\sigma(b_n) \in \sigma(I)\sigma(J)$. Thus $\sigma(IJ) \subseteq \sigma(I)\sigma(J)$, and applying the same argument to $\sigma(I), \sigma(J)$, and σ^{-1} implies $\sigma^{-1}(\sigma(I)\sigma(J)) \subseteq IJ$ and therefore $\sigma(I)\sigma(J) \subseteq \sigma(IJ)$. Thus $\sigma(IJ) = \sigma(I)\sigma(J)$ for all $I, J \in \mathcal{I}_B$ and the G-action on $\mathcal{I}_B$ commutes with its group operation.

Let $\mathfrak{p}$ be a prime of B and let $\sigma(\mathfrak{p}) = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_n^{e_n}$ be the unique factorization of $\sigma(\mathfrak{p})$ in the Dedekind domain B. Applying σ^{-1} to both sides yields $\mathfrak{p} = \sigma^{-1}(\mathfrak{q}_1)^{e_1} \cdots \sigma^{-1}(\mathfrak{q}_n)^{e_n}$, which implies $n = 1$ and $e_1 = 1$, since $\mathfrak{p}$ is prime, so $\sigma(\mathfrak{p}) = \mathfrak{q}_1$ is prime. □

Recall that by a prime of A (or K) we mean a nonzero prime ideal of A, and similarly for B (and L), and for any prime $\mathfrak{p}$ of A we use $\{\mathfrak{q}|\mathfrak{p}\}$ to denote the set of primes $\mathfrak{q}$ that lie above $\mathfrak{p}$ (divide $\mathfrak{p}B$, equivalently, for which $\mathfrak{q} = A \cap \mathfrak{p}$).

Corollary 7.2. *Assume AKLBG and let $\mathfrak{p}$ be a prime of A. The group G acts transitively on the set $\{\mathfrak{q}|\mathfrak{p}\}$.*

Proof. Consider any $\sigma \in G$. For $\mathfrak{q}|\mathfrak{p}$ we have $\mathfrak{p}B \subseteq \mathfrak{q}$ and $\sigma(\mathfrak{p}B) \subseteq \sigma(\mathfrak{q})$, so $\sigma(\mathfrak{q})|\mathfrak{p}$ (in a Dedekind domain, to contain is to divide). Thus $\{\mathfrak{q}|\mathfrak{p}\}$ is closed under the action of G, we just need to show that it consists of a single orbit.

If $\{\mathfrak{q}|\mathfrak{p}\} = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$ contains more than one G-orbit, we may assume WLOG that $\mathfrak{q}_1$ and $\mathfrak{q}_2$ lie in distinct G-orbits. The primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ are maximal ideals, hence pairwise coprime, so the CRT gives us a ring isomorphism

$$\frac{B}{\mathfrak{q}_1 \cdots \mathfrak{q}_n} \simeq \frac{B}{\mathfrak{q}_1} \times \cdots \times \frac{B}{\mathfrak{q}_n},$$

and we may choose $b \in B$ so that $b \equiv 0 \bmod \mathfrak{q}_2$ and $b \equiv 1 \bmod \sigma^{-1}(\mathfrak{q}_1)$ for all $\sigma \in G$ (by hypothesis, $\sigma(\mathfrak{q}_2) \neq \mathfrak{q}_1$ for all $\sigma \in G$, since $\mathfrak{q}_1, \mathfrak{q}_2$ lie in different G-orbits). Then $b \in \mathfrak{q}_2$ and

$$N_{L/K}(b) = \prod_{\sigma \in G} \sigma(b) \equiv 1 \bmod \mathfrak{q}_1,$$

so $N_{L/K}(b) \notin A \cap \mathfrak{q}_1 = \mathfrak{p}$. But $N_{L/K}(b) \in N_{L/K}(\mathfrak{q}_2) = \mathfrak{p}^{f_{\mathfrak{q}_2}} \subseteq \mathfrak{p}$, a contradiction. □

For each $\sigma \in G = \mathrm{Gal}(L/K)$, we have $\sigma(B) = B$, thus σ restricts to a ring automorphism of B that fixes elements of the subring $A \subseteq K$, and in particular, elements of the prime $\mathfrak{p}$. It follows that σ induces a field isomorphism $\bar{\sigma} \in \mathrm{Hom}_{A/\mathfrak{p}}(B/\mathfrak{q}, B/\sigma(\mathfrak{q}))$ that for each $a \in b$ sends $\bar{a} := a + \mathfrak{q} \in B/\mathfrak{q}$ to $\bar{\sigma}(\bar{a}) := \sigma(a + \mathfrak{q}) = a + \sigma(\mathfrak{q}) \in B/\sigma(\mathfrak{q})$.

Corollary 7.3. *Assume AKLBG and let $\mathfrak{p}$ be a prime of A. The residue field degree $f_{\mathfrak{q}} = [B/\mathfrak{q} : A/\mathfrak{p}]$ and ramification index $e_{\mathfrak{q}} = v_{\mathfrak{q}}(\mathfrak{p}B)$ are the same for every $\mathfrak{q}|\mathfrak{p}$.*

Proof. For each $\sigma \in G$ the induced isomorphism $\bar{\sigma} \in \mathrm{Hom}_{A/\mathfrak{p}}(B/\mathfrak{q}, B/\sigma(\mathfrak{q}))$ implies $f_{\mathfrak{q}} = f_{\sigma(\mathfrak{q})}$, and since G acts transitively on $\{\mathfrak{q}|\mathfrak{p}\}$, the $f_{\mathfrak{q}}$ must all coincide.

For each $\sigma \in G$ we also have $\sigma(\mathfrak{p}) = \mathfrak{p}$ and $\sigma(B) = B$, so $\sigma(\mathfrak{p}B) = \mathfrak{p}B$, and for each $\mathfrak{q}|\mathfrak{p}$,

$$e_{\mathfrak{q}} = v_{\mathfrak{q}}(\mathfrak{p}B) = v_{\mathfrak{q}}(\sigma(\mathfrak{p}B))) = v_{\mathfrak{q}}\Big(\sigma\Big(\prod_{\mathfrak{r}|\mathfrak{p}} \mathfrak{r}^{e_{\mathfrak{r}}}\Big)\Big) = v_{\mathfrak{q}}\Big(\prod_{\mathfrak{r}|\mathfrak{p}} \sigma(\mathfrak{r})^{e_{\mathfrak{r}}}\Big) = v_{\mathfrak{q}}\Big(\prod_{\mathfrak{r}|\mathfrak{p}} \mathfrak{r}^{e_{\sigma^{-1}(\mathfrak{r})}}\Big) = e_{\sigma^{-1}(\mathfrak{q})}.$$

Since G acts transitively on $\{\mathfrak{q}|\mathfrak{p}\}$, the $e_{\mathfrak{q}}$ must all coincide. □

The corollary implies that whenever L/K is Galois, we may unambiguously write $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$ instead of $e_{\mathfrak{q}}$ and $f_{\mathfrak{q}}$, and recall that we previously defined $g_{\mathfrak{p}} := \#\{\mathfrak{q}|\mathfrak{p}\}$.

Corollary 7.4. *Assume AKLBG. For each prime $\mathfrak{p}$ of A we have $e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}} = [L : K]$.*

Proof. This follows immediately from Theorem 5.34 and Corollary 7.3. □

Example 7.5. Assume *AKLBG*. When $n := [L\!:\!K]$ is prime there are just three ways a prime $\mathfrak{p}$ of A can split in B:

- $e_{\mathfrak{p}} = n$ and $f_{\mathfrak{p}} = g_{\mathfrak{p}} = 1$, in which case $\mathfrak{p}$ is totally ramified;
- $f_{\mathfrak{p}} = n$ and $e_{\mathfrak{p}} = g_{\mathfrak{p}} = 1$, in which case $\mathfrak{p}$ is inert;
- $g_{\mathfrak{p}} = n$ and $e_{\mathfrak{p}} = f_{\mathfrak{p}} = 1$, in which case $\mathfrak{p}$ splits completely.

7.2 Decomposition and inertia groups

Definition 7.6. Assume $AKLBG$ and let $\mathfrak{q}$ be a prime of B. The *decomposition group* of $\mathfrak{q}$ is the stabilizer of $\mathfrak{q}$ in G, denoted $D_{\mathfrak{q}} = D_{\mathfrak{q}}(L/K)$.

Lemma 7.7. *Assume $AKLBG$ and let $\mathfrak{p}$ be a prime of A. The decomposition groups $D_{\mathfrak{q}}$ for $\mathfrak{q}|\mathfrak{p}$ are all conjugate in G, with $\#D_{\mathfrak{q}} = e_{\mathfrak{p}}f_{\mathfrak{p}}$ and $[G : D_{\mathfrak{q}}] = g_{\mathfrak{p}}$.*

Proof. Points in the same orbit of group action have conjugate stabilizers; Corollary 7.2 thus implies that for all $\mathfrak{q}|\mathfrak{p}$ the $D_{\mathfrak{q}}$ are conjugate. The orbit-stabilizer theorem implies $[G : D_{\mathfrak{q}}] = \#\{\mathfrak{q}|\mathfrak{p}\} = g_{\mathfrak{p}}$. We have $\#G = [L : K] = e_{\mathfrak{p}}f_{\mathfrak{p}}g_{\mathfrak{p}}$, by Corollary 7.4, therefore $\#D_{\mathfrak{q}} = \#G/[G : D_{\mathfrak{q}}] = e_{\mathfrak{p}}f_{\mathfrak{p}}g_{\mathfrak{p}}/g_{\mathfrak{p}} = e_{\mathfrak{p}}f_{\mathfrak{p}}$. □

Let us now consider a particular prime $\mathfrak{q}|\mathfrak{p}$ of B (lying above $\mathfrak{p} := \mathfrak{q} \cap A$). For each $\sigma \in G$ we have a field isomorphism $\bar{\sigma} \in \operatorname{Hom}_{A/\mathfrak{p}}(B/\mathfrak{q}, B/\sigma(\mathfrak{q}))$ defined by $\bar{\sigma}(\bar{a}) := \overline{\sigma(a)}$ for all $a \in B$, where $\bar{a}$ denotes the image of a in $B/\mathfrak{q}$. In the special case $\sigma \in D_{\mathfrak{q}}$, we have $\sigma(\mathfrak{q}) = \mathfrak{q}$ and $\bar{\sigma} \in \operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q})$. The map $\sigma \mapsto \overline{\sigma}$ defines a group homomorphism $\pi_{\mathfrak{q}} \colon D_{\mathfrak{q}} \to \operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q})$, since for any $a \in B$ we have

$$\overline{\sigma\tau}(\bar{a}) = \overline{\sigma\tau(a)} = \overline{\sigma(\tau(a))} = \overline{\sigma}(\overline{\tau(a)}) = \overline{\sigma}(\overline{\tau}(\bar{a})).$$

Proposition 7.8. *Assume $AKLBG$ and let $\mathfrak{q}|\mathfrak{p}$ be a prime of B. The residue field extension $(B/\mathfrak{q})/(A/\mathfrak{p})$ is normal and the homomorphism $\pi_{\mathfrak{q}} \colon D_{\mathfrak{q}} \to \operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q})$ is surjective.*

Proof. Let F be the separable closure of $A/\mathfrak{p}$ in $B/\mathfrak{q}$, so that restriction to F induces an isomorphism $\operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q}) \xrightarrow{\sim} \operatorname{Gal}(F/(A/\mathfrak{p})))$. Since F is a finite separable extension of $A/\mathfrak{p}$, the primitive element theorem implies that $F = (A/\mathfrak{p})(\alpha)$ for some $\alpha \in F^{\times}$. Let us now pick $a \in B$ such that $a \equiv \alpha \bmod \mathfrak{q}$ and $a \equiv 0 \bmod \sigma^{-1}(\mathfrak{q})$ (so $\sigma(a) \equiv 0 \bmod \mathfrak{q}$) for all $\sigma \in G - D_{\mathfrak{q}}$; the CRT implies that such an a since for $\sigma \in G - D_{\mathfrak{q}}$ the ideals $\mathfrak{q}$ and $\sigma(\mathfrak{q})$ are distinct and therefore coprime (since they are maximal ideals). Now define

$$g(x) := \prod_{\sigma \in G} \big(x - \sigma(a)\big) \in A[x],$$

and let $\overline{g}$ denote the image of g in $(A/\mathfrak{p})[x]$, with roots $\{\overline{\sigma}(\alpha) : \sigma \in G\}$. For each $\sigma \in G - D_{\mathfrak{q}}$ we have $\overline{\sigma}(\bar{a}) = 0$, so 0 is a root of $\overline{g}(x)$ with multiplicity at least $m = \#(G - D_{\mathfrak{q}})$, and the remaining roots are $\overline{\sigma}(\alpha)$ for $\sigma \in D_{\mathfrak{q}}$; these are all Galois conjugates of α in $B/\mathfrak{q}$. It follows that $\overline{g}(x)/x^m$ divides a power of the minimal polynomial of α, but the minimal polynomial of α is irreducible in $(A/\mathfrak{p})[x]$, so $\overline{g}(x)/x^m$ is equal to a power of the minimal polynomial of α, and this means that every $\operatorname{Gal}(F/(A/\mathfrak{p}))$-conjugate of α has the form $\overline{\sigma}(\alpha)$ for some $\sigma \in D_{\mathfrak{q}}$. It follows that $D_{\mathfrak{q}}$ surjects onto $\operatorname{Gal}(F/(A/\mathfrak{p})) \simeq \operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q})$ and $\pi_{\mathfrak{q}}$ is surjective.

To show that $B/\mathfrak{q}$ is a normal extension of $A/\mathfrak{p}$ it suffices to show that each $\overline{a} \in B/\mathfrak{q}$ is the root of a monic polynomial in $(A/\mathfrak{p})[x]$ that splits completely in $(B/\mathfrak{q})[x]$. For each $a \in B$, we can define $g \in A[x]$ and $\overline{g} \in (A/\mathfrak{p})[x]$ as above, showing that each $\bar{a} \in B/\mathfrak{q}$ is a root of the monic polynomial $\overline{g}$, which splits completely in $(B/\mathfrak{q})[x]$ as desired. □

Definition 7.9. Assume $AKLBG$, and let $\mathfrak{q}|\mathfrak{p}$ be a prime of B. The kernel of the surjective homomorphism $\pi_{\mathfrak{q}} \colon D_{\mathfrak{q}} \to \operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q})$ is the *inertia group* $I_{\mathfrak{q}}$ of $\mathfrak{q}$.

Corollary 7.10. *Assume $AKLBG$ and let $\mathfrak{q}|\mathfrak{p}$ be a prime of B. We have an exact sequence*

$$1 \longrightarrow I_{\mathfrak{q}} \longrightarrow D_{\mathfrak{q}} \longrightarrow \operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q}) \longrightarrow 1,$$

and $\#I_{\mathfrak{q}} = e_{\mathfrak{p}}[B/\mathfrak{q} : A/\mathfrak{p}]_i$.

We have shown that the residue field $B/\mathfrak{q}$ is always a normal extension of the residue field $A/\mathfrak{p}$. Let us now suppose that it is also separable, hence Galois; this holds, for example, if $A/\mathfrak{p}$ is a perfect field, and in particular, whenever $A/\mathfrak{p}$ is a finite field. We then have

$$D_\mathfrak{q}/I_\mathfrak{q} \simeq \operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q}) = \operatorname{Gal}((B/q)/(A/\mathfrak{p})).$$

Proposition 7.11. *Assume AKLBG, let $\mathfrak{q}|\mathfrak{p}$ be a prime of B, and suppose $B/\mathfrak{q}$ is a separable extension of $A/\mathfrak{p}$. We have a tower of field extensions $K \subseteq L^{D_\mathfrak{q}} \subseteq L^{I_\mathfrak{q}} \subseteq L$ with*

$$\begin{aligned} e_\mathfrak{p} &= [L : L^{I_\mathfrak{q}}] = \#I_\mathfrak{q};\\ f_\mathfrak{p} &= [L^{I_\mathfrak{q}} : L^{D_\mathfrak{q}}] = \#D_\mathfrak{q}/\#I_\mathfrak{q};\\ g_\mathfrak{p} &= [L^{D_\mathfrak{q}} : K] = \#\{\mathfrak{q}|\mathfrak{p}\}.\end{aligned}$$

The fields $L^{D_\mathfrak{q}}$ and $L^{I_\mathfrak{q}}$ are the *decomposition field* and *inertia field* associated to $\mathfrak{q}$.

Proof. The third equality follows immediately from Lemma 7.7. The second follows from Proposition 7.8 and the separability of $(B/\mathfrak{q})/A/\mathfrak{p})$, since $D_\mathfrak{q}/I_\mathfrak{q} \simeq \operatorname{Gal}((B/\mathfrak{q})/(A/\mathfrak{p}))$ has cardinality $f_\mathfrak{p} = [B/\mathfrak{q} \colon A/\mathfrak{p}]$. We then have $[L : L^{D_\mathfrak{q}}] = \#D_\mathfrak{q} = e_\mathfrak{p} f_\mathfrak{p}$ and $\#D_\mathfrak{q}/\#I_\mathfrak{q} = f_\mathfrak{p}$, so $\#I_q = e_\mathfrak{p}$, so the first equality also holds. □

We now consider an intermediate field E lying between K and L. Let us fix a prime $\mathfrak{q}|\mathfrak{p}$ of B, and let $\mathfrak{q}_E \coloneqq \mathfrak{q} \cap E$, so that $\mathfrak{q}|\mathfrak{q}_E$ and $\mathfrak{q}_E|\mathfrak{p}$, and let us use $\overline{G}_\mathfrak{q}(L/K) \coloneqq \operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q})$, $\overline{G}_\mathfrak{q}(L/E) \coloneqq \operatorname{Aut}_{(B\cap E)/\mathfrak{q}_E}(B/\mathfrak{q})$, $\overline{G}_{\mathfrak{q}_E}(E/K) \coloneqq \operatorname{Aut}_{A/\mathfrak{p}}((B \cap E)/\mathfrak{q}_E)$ to denote the automorphism groups of the residue field extensions associated to the tower $K \subseteq E \subseteq L$. We use the notation $D_\mathfrak{q}(L/E)$ to denote the decomposition group of $\mathfrak{q}$ relative to the extension L/E (note that L/E is Galois since L/K is), and similarly define $D_\mathfrak{q}(L/K)$, as well as $I_\mathfrak{q}(L/E)$ and $I_\mathfrak{q}(L/K)$. In the case that E/K is also Galois, we similarly use $D_{\mathfrak{q}_E}(E/K)$ and $I_{\mathfrak{q}_E}(E/K)$ to denote the decomposition and inertia group of $\mathfrak{q}_E$ (subgroups of $\operatorname{Gal}(E/K)$).

Proposition 7.12. *Assume AKLBG, let E be an intermediate field between K and L. Let $\mathfrak{q}$ be a prime of B and let $\mathfrak{q}_E = \mathfrak{q} \cap E$ and $\mathfrak{p} = \mathfrak{q} \cap K$. Then*

$$D_\mathfrak{q}(L/E) = D_\mathfrak{q}(L/K) \cap \operatorname{Gal}(L/E) \qquad \textit{and} \qquad I_\mathfrak{q}(L/E) = I_\mathfrak{q}(L/K) \cap \operatorname{Gal}(L/E).$$

If E/K is Galois, then we have the following commutative diagram of exact sequences:

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & I_\mathfrak{q}(L/E) \arrow[r] \arrow[d] & I_\mathfrak{q}(L/K) \arrow[r] \arrow[d] & I_{\mathfrak{q}_E}(E/K) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & D_\mathfrak{q}(L/E) \arrow[r] \arrow[d] & D_\mathfrak{q}(L/K) \arrow[r] \arrow[d] & D_{\mathfrak{q}_E}(E/K) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \overline{G}_\mathfrak{q}(L/E) \arrow[r] \arrow[d] & \overline{G}_\mathfrak{q}(L/K) \arrow[r] \arrow[d] & \overline{G}_{\mathfrak{q}_E}(E/K) \arrow[r] \arrow[d] & 1 \\
 & 1 & 1 & 1 &
\end{tikzcd}$$

Proof. Note that $D_{\mathfrak{q}}(L/E) \subseteq \mathrm{Gal}(L/E) \subseteq \mathrm{Gal}(L/K)$. An element σ of $\mathrm{Gal}(L/K)$ lies in $D_{\mathfrak{q}}(L/E)$ if and only if it fixes E (hence lies in $\mathrm{Gal}(L/E)$) and satisfies $\sigma(\mathfrak{q}) = \mathfrak{q}$ (hence lies in $D_{\mathfrak{q}}(L/K)$), which proves the first claim. For the second claim, the restriction of $\pi_{\mathfrak{q}}(L/K)\colon D_{\mathfrak{q}}(L/K) \to \overline{G}_{\mathfrak{q}}(L/K)$ to $D_{\mathfrak{q}}(L/E)$ is the map $\pi_{\mathfrak{q}}(L/E)\colon D_{\mathfrak{q}}(L/E) \to \overline{G}_{\mathfrak{q}}(L/E)$, hence the kernels agree after intersecting with $\mathrm{Gal}(L/E)$.

The exactness of the columns follows from Corollary 7.10; we now argue exactness of the rows. Each row corresponds to an inclusion followed be a restriction in which the inclusion is precisely the kernel of the restriction (for the first two rows this follows from the two claims proved above and for the third row it follows from the main theorem of Galois theory); exactness at the first two groups in each row follows. Surjectivity of the restriction maps follows from the bijection used in the proof of Lemma 4.10. We have a bijection $\mathrm{Hom}_K(L,\Omega) \to \mathrm{Hom}_E(L,\Omega) \times \mathrm{Hom}_K(E,\Omega)$ whose second factor is restriction, and we may view this as a bijection $\phi\colon \mathrm{Gal}(L,K) \to \mathrm{Gal}(L/E) \times \mathrm{Gal}(E/K)$. If $\sigma \in \mathrm{Gal}(E/K)$ stabilizes $\mathfrak{q}_E$ then $\phi^{-1}(1,\sigma) \in \mathrm{Gal}(L/K)$ stabilizes $\mathfrak{q}$ and restricts to σ; this implies surjectivity of the restriction maps in the first two rows, and for the third we replace $L/E/K$ with the corresponding tower of residue field extensions (and forget about stabilizing $\mathfrak{q}_E$).

We now argue commutativity of the four corner squares which suffices to prove the commutativity of the enitre diagram. The upper left square commutes because all the maps are inclusions. The upper right square commutes because inclusion and restriction commute. The lower left square commutes because the horizontal maps are inclusions and the vertical maps coincide on $D_{\mathfrak{q}}(L/E)$. The lower right square commutes because the horizontal maps are restrictions and the vertical maps agree after restriction to E. □

7.3 Frobenius elements

We now add the further assumption that the residue fields $A/\mathfrak{p}$ (and therefore $B/\mathfrak{q}$) are finite for all primes $\mathfrak{p}$ of K.[1] This holds, for example, whenever K is a global field (a finite extension of $\mathbb{Q}$ or $\mathbb{F}_q(t)$). In this situation $B/\mathfrak{q}$ is necessarily a Galois extension of $A/\mathfrak{p}$ (we don't even need Proposition 7.8 for this, finite extensions of finite fields are always normal, in addition to being separable).

In order to simplify the notation, when working with finite residue fields we may write $\mathbb{F}_{\mathfrak{q}} := B/\mathfrak{q}$ and $\mathbb{F}_{\mathfrak{p}} := A/\mathfrak{p}$; these are finite fields of p-power order, where p is the characteristic of $\mathbb{F}_{\mathfrak{p}}$ (and of $\mathbb{F}_{\mathfrak{q}}$). Note that the field K (and L) need not have characteristic p (consider the case of number fields), but if the characteristic of K is positive then it must be p (consider the homomorphism $A \to A/\mathfrak{p}$ from the integral domain A to the field $A/\mathfrak{p}$).

Let $\mathfrak{q}|\mathfrak{p}$ be a prime of B. Corollary 7.10 gives us an exact sequence

$$1 \longrightarrow I_{\mathfrak{q}} \longrightarrow D_{\mathfrak{q}} \xrightarrow{\pi_{\mathfrak{q}}} \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}) \longrightarrow 1.$$

If $\mathfrak{p}$ (equivalently, $\mathfrak{q}$) is unramified, then $e_{\mathfrak{p}} = e_{\mathfrak{q}} = 1$ and $I_{\mathfrak{q}}$ is trivial. In this case we have an isomorphism

$$\pi_{\mathfrak{q}}\colon D_{\mathfrak{q}} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}).$$

The Galois group $\mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$ is the cyclic group of order $f_{\mathfrak{p}} = [\mathbb{F}_{\mathfrak{q}} : \mathbb{F}_{\mathfrak{p}}]$ generated by the *Frobenius automorphism*

$$x \mapsto x^{\#\mathbb{F}_{\mathfrak{p}}}.$$

[1] There exist Dedekind domains A (PIDs even) with a mixture of finite and infinite residue fields; see [1].

Note that the cardinality $\#\mathbb{F}_\mathfrak{p}$ of the finite field $\mathbb{F}_\mathfrak{p}$ is necessarily a power of its characteristic p. If $K = \mathbb{Q}$ and $\mathfrak{p} = (p)$ is a prime of $\mathbb{Z}$, then $\mathbb{F}_\mathfrak{p} = \mathbb{Z}/p\mathbb{Z}$ is the field with p elements, but in general the field $\mathbb{F}_\mathfrak{p}$ need not be a prime field (consider $K = \mathbb{Q}(i)$ and $\mathfrak{p} = (7)$).

Definition 7.13. Assume *AKLBG* with finite residue fields and $\mathfrak{q}|\mathfrak{p}$ unramified. The inverse image of the Frobenius automorphism of $\mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ under $\pi_\mathfrak{q} : D_\mathfrak{q} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ is the *Frobenius element* $\sigma_\mathfrak{q} \in D_\mathfrak{q} \subseteq G$ (also called the *Frobenius substitution* [2, §8]).

Proposition 7.14. *Assume AKLBG with finite residue fields and* $\mathfrak{q}|\mathfrak{p}$ *unramified. The Frobenius element* $\sigma_\mathfrak{q}$ *is the unique* $\sigma \in G$ *such that for all* $x \in B$ *we have*

$$\sigma(x) \equiv x^{\#\mathbb{F}_\mathfrak{p}} \bmod \mathfrak{q}.$$

Proof. Clearly $\sigma_\mathfrak{q}$ has this property, we just need to show uniqueness. Suppose $\sigma \in G$ has the desired property. For any $x \in \mathfrak{q}$ we have $x \equiv 0 \bmod \mathfrak{q}$, and $\sigma(x) \equiv x^{\#\mathbb{F}_\mathfrak{p}} \bmod \mathfrak{q}$ implies $\sigma(x) \equiv 0 \bmod \mathfrak{q}$, so $\sigma(x) \in \mathfrak{q}$; it follows that $\sigma(\mathfrak{q}) = \mathfrak{q}$, and therefore $\sigma \in D_\mathfrak{q}$. The isomorphism $\pi_\mathfrak{q} \colon D_\mathfrak{q} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ maps both σ and $\sigma_\mathfrak{q}$ to the Frobenius automorphism $x \mapsto x^{\#\mathbb{F}_\mathfrak{p}}$, so we must have $\sigma = \sigma_\mathfrak{q}$. □

Proposition 7.15. *Assume AKLBG with finite residue fields and* $\mathfrak{q}|\mathfrak{p}$ *unramified. For all* $\mathfrak{q}'|\mathfrak{p}$ *the Frobenius elements* $\sigma_\mathfrak{q}$ *and* $\sigma_{\mathfrak{q}'}$ *are conjugate in* G.

Proof. By Corollary 7.2, G acts transitively on $\{\mathfrak{q}|\mathfrak{p}\}$, so let $\tau \in G$ be such that $\mathfrak{q}' = \tau(\mathfrak{q})$. For any $x \in B$ we have

$$\begin{aligned}
\sigma_\mathfrak{q}(x) &\equiv x^{\#\mathbb{F}_\mathfrak{p}} \bmod \mathfrak{q}. \\
\tau(\sigma_\mathfrak{q}(x)) &\equiv \tau\left(x^{\#\mathbb{F}_\mathfrak{p}}\right) \bmod \tau(\mathfrak{q}) \\
(\tau\sigma_\mathfrak{q})(x) &\equiv \tau(x)^{\#\mathbb{F}_\mathfrak{p}} \bmod \mathfrak{q}' \\
(\tau\sigma_\mathfrak{q})(\tau^{-1}(x)) &\equiv \tau(\tau^{-1}(x))^{\#\mathbb{F}_\mathfrak{p}} \bmod \mathfrak{q}' \\
(\tau\sigma_\mathfrak{q}\tau^{-1})(x) &\equiv x^{\#\mathbb{F}_\mathfrak{p}} \bmod \mathfrak{q}',
\end{aligned}$$

where we applied τ to both sides in the second line and replaced x by $\tau^{-1}(x)$ in the fourth line. The uniqueness of $\sigma_{\mathfrak{q}'}$ given by Proposition 7.14 implies $\sigma_{\mathfrak{q}'} = \tau\sigma_\mathfrak{q}\tau^{-1}$. □

Definition 7.16. Assume *AKLBG* with finite residue fields and $\mathfrak{q}|\mathfrak{p}$ unramified. The conjugacy class of the Frobenius element $\sigma_\mathfrak{q} \in G$ is the *Frobenius class* of $\mathfrak{p}$, denoted $\mathrm{Frob}_\mathfrak{p}$.

It is common to abuse terminology and refer to $\mathrm{Frob}_\mathfrak{p}$ as a Frobenius element $\sigma_\mathfrak{p} \in G$ representing its conjugacy class (so $\sigma_\mathfrak{p} = \sigma_\mathfrak{q}$ for some $\mathfrak{q}|\mathfrak{p}$); there is little risk of confusion so long as we remember that $\sigma_\mathfrak{p}$ is only determined up to conjugacy (which usually governs all the properties we care about). There is, however, one situation where this terminology is entirely correct. If G is abelian then its conjugacy classes all consist of a single element, in which we case $\mathrm{Frob}_\mathfrak{p} = \{\sigma_\mathfrak{q} : \mathfrak{q}|\mathfrak{p}\}$ is a singleton set and there is a unique choice for $\sigma_\mathfrak{p}$ (note that $\#\{\sigma_\mathfrak{q} : \mathfrak{q}|\mathfrak{p}\} = 1$ does not imply $\#\{\mathfrak{q}|\mathfrak{p}\} = 1$, the map $\mathfrak{q} \to \sigma_\mathfrak{q}$ need not be injective).

7.4 Artin symbols

There is another notation commonly used to denote Frobenius elements that includes the field extension in the notation.

Definition 7.17. Assume $AKLBG$ with finite residue fields. For each unramified prime $\mathfrak{q}$ of L we define the *Artin symbol*

$$\left(\frac{L/K}{\mathfrak{q}}\right) := \sigma_{\mathfrak{q}}.$$

Proposition 7.18. *Assume $AKLBG$ with finite residue fields and $\mathfrak{q}|\mathfrak{p}$ unramified. Then $\mathfrak{p}$ splits completely if and only if $\left(\frac{L/K}{\mathfrak{q}}\right) = 1$.*

Proof. This follows directly from the definitions: if $\mathfrak{p}$ splits completely then $e_{\mathfrak{p}} f_{\mathfrak{p}} = 1$ and $D_{\mathfrak{q}} = \langle \sigma_{\mathfrak{q}} \rangle = \{1\}$. Conversely, if $D_{\mathfrak{q}} = \langle \sigma_{\mathfrak{q}} \rangle = \{1\}$ then $e_{\mathfrak{p}} f_{\mathfrak{p}} = 1$ and $\mathfrak{p}$ splits completely. □

We will see later in the course that the extension L/K is completely determined by the set of primes $\mathfrak{p}$ that split completely in L. Thus in some sense the Artin symbol captures the essential structure of L/K.

Proposition 7.19. *Assume $AKLBG$ with finite residue fields and let $\mathfrak{q}|\mathfrak{p}$ be unramified. Let E be an intermediate field between K and L, and define $\mathfrak{q}_E := \mathfrak{q} \cap E$. Then*

$$\left(\frac{L/E}{\mathfrak{q}}\right) = \left(\frac{L/K}{\mathfrak{q}}\right)^{[\mathbb{F}_{\mathfrak{q}_E}:\mathbb{F}_{\mathfrak{p}}]},$$

and if E/K is Galois then $\left(\frac{E/K}{\mathfrak{q}_E}\right)$ is the restriction of $\left(\frac{L/K}{\mathfrak{q}}\right)$ to E.

Proof. For the first claim, note that $\#\mathbb{F}_{\mathfrak{q}_E} = (\#\mathbb{F}_{\mathfrak{p}})^{[\mathbb{F}_{\mathfrak{q}_E}:\mathbb{F}_{\mathfrak{p}}]}$. The second claim follows from the commutativity of the lower right square in the commutative diagram of Proposition 7.12: the Frobenius automorphism $x \mapsto x^{\#\mathbb{F}_{\mathfrak{p}}}$ of $\operatorname{Gal}(\mathbb{F}_{\mathfrak{q}_E}/\mathbb{F}_{\mathfrak{p}})$ is the restriction of the Frobenius automorphism $x \mapsto x^{\#\mathbb{F}_{\mathfrak{p}}}$ of $\operatorname{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$ to $\mathbb{F}_{\mathfrak{q}_E}$. □

When L/K is abelian, the Artin symbol takes the same value for all $\mathfrak{q}|\mathfrak{p}$ and we may instead write

$$\left(\frac{L/K}{\mathfrak{p}}\right) := \sigma_{\mathfrak{p}} := \sigma_{\mathfrak{q}},$$

where $\mathfrak{q}$ is any primitive above $\mathfrak{p}$. In this setting we now view the Artin symbol as a function mapping unramified primes $\mathfrak{p}$ to Frobenius elements $\sigma_{\mathfrak{p}} \in G$. We wish to extend this map to a multiplicative homomorphism from the ideal group $\mathcal{I}_A$ to the Galois group $G = \operatorname{Gal}(L/K)$, but ramified primes $\mathfrak{q}|\mathfrak{p}$ cause problems: the homomorphism $\pi_{\mathfrak{q}}\colon D_{\mathfrak{q}} \to \operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_{\mathfrak{p}})$ is not a bijection when $\mathfrak{p}$ is ramified (it has nontrivial kernel I_q of order $e_{\mathfrak{q}} = e_{\mathfrak{p}} > 1$).

For any set S of primes of A, let I_A^S denote the subgroup of $\mathcal{I}_A$ generated by the primes of A that do not lie in S (a free abelian group).

Definition 7.20. Let A be a Dedekind domain with finite residue fields. Let L be a finite abelian extension of $K = \operatorname{Frac} A$, and let S be the set of primes of A that ramify in L. The *Artin map* is the homomorphism

$$\begin{aligned} \left(\frac{L/K}{\cdot}\right) : \mathcal{I}_A^S &\to \operatorname{Gal}(L/K) \\ \prod_{i=1}^m \mathfrak{p}_i^{e_i} &\mapsto \prod_{i=1}^m \left(\frac{L/K}{\mathfrak{p}_i}\right)^{e_i}. \end{aligned}$$

Remark 7.21. We will prove in later lectures that the set S of ramified primes is finite, but the definition makes sense in any case.

One of the main results of class field theory is that the Artin map is surjective (this is part of what is known as *Artin reciprocity*). This is a deep theorem that we are not yet ready to prove, but we can verify that it holds in some simple examples.

Example 7.22 (Quadratic fields)**.** Let $K=\mathbb{Q}$ and $L=\mathbb{Q}(\sqrt{d})$ for some square-free integer $d\neq 1$. Then $\operatorname{Gal}(L/K)$ has order 2 and is certainly abelian. As you proved on Problem Set 2, the only ramified primes $\mathfrak{p}=(p)$ of $A=\mathbb{Z}$ are those that divide the *discriminant*

$$D\coloneqq \operatorname{disc}(L/K)=\begin{cases} d & \text{if } d\equiv 1 \bmod 4,\\ 4d & \text{if } d\not\equiv 1 \bmod 4.\end{cases}$$

If we identify $\operatorname{Gal}(L/K)$ with the multiplicative group $\{\pm 1\}$, then

$$\left(\frac{L/K}{\mathfrak{p}}\right)=\left(\frac{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}{(p)}\right)=\left(\frac{D}{p}\right)=\pm 1,$$

where $(\frac{D}{p})$ is the *Kronecker symbol*. For odd primes $p\nmid D$ we have

$$\left(\frac{D}{p}\right)=\begin{cases} +1 & \text{if } D \text{ is a nonzero square modulo } p,\\ -1 & \text{if } D \text{ is not a square modulo } p,\end{cases}$$

and for $p=2$ not dividing D (in which case $D=d\equiv 1 \bmod 4$) we have

$$\left(\frac{D}{2}\right)=\begin{cases} +1 & \text{if } D\equiv 1 \bmod 8,\\ -1 & \text{if } D\equiv 5 \bmod 8.\end{cases}$$

The cyclotomic extensions $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ provide another interesting example that you will have an opportunity to explore on Problem Set 4.

References

[1] R. C. Heitmann, *PID's with specified residue fields*, Duke Math. J. **41** (1974), 565–582.

[2] J.-P. Serre, *Local fields*, Springer, 1979.

18.785 Number Theory I
Fall 2017