18.785 Number theory I **Fall 2016**
Lecture #7 **9/29/2016**

7 Galois extensions, Frobenius elements, the Artin map

In our standard $AKLB$ setup the finite extension L/K is separable but not necessarily normal. We now add the additional hypothesis that L/K is normal so that L/K is a Galois extension, and let $G := \operatorname{Gal}(L/K)$ denote the Galois group. We will use the shorthand $AKLBG$ 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. Then G acts on the ideal group $\mathcal{I}_B$ of B via*

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

This action commutes with the group operation in $\mathcal{I}_B$ and permutes the primes of B.

Proof. Let $\sigma \in G$. We first show $\sigma(B) = B$: each $b \in B$ is integral over A, hence the root of some monic polynomial $f \in A[x] \subset K[x]$ whose coefficients are fixed by σ. We have $f(b) = 0$, thus $\sigma(f(b)) = f(\sigma(b)) = 0$ and $\sigma(b) \in L$ is integral over A and therefore lies in B, the integral closure of A in L; this proves $\sigma(B) \subseteq B$. By the same argument, $\sigma^{-1}(B) \subseteq B$, so $B \subseteq \sigma(B)$ and therefore $\sigma(B) = B$.

Now let I be an ideal of B. Then $\sigma(I) \subseteq \sigma(B) = B$. The set $\sigma(I)$ is closed under addition, since σ is a field automorphism, and if $a \in I$ and $b \in B$ then $\sigma^{-1}(b) \in B$ and $\sigma^{-1}(b)a \in I$, thus $b\sigma(a) \in \sigma(I)$. It follows that $\sigma(I)$ is an ideal of B, and we note that $\sigma(I) = (0)$ if and only if $I = (0)$.

Each nonzero fractional ideal has the form xI for some $x \in L^\times$ and nonzero ideal I. We have $\sigma(xI) = \sigma(x)\sigma(I)$, which is a nonzero fractional ideal of B, since $\sigma(x) \in L^\times$ and $\sigma(I)$ is an ideal. Thus each $\sigma \in G$ permutes the set $\mathcal{I}_B$. The identity automorphism clearly acts trivially, and for any $\sigma, \tau \in G$ and $I \in \mathcal{I}_B$ we have

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

thus the group G acts on the set $\mathcal{I}_B$.

Now let $I, J \in \mathcal{I}_B$ and $\sigma \in G$. We have $x = a_1b_1 + \cdots + a_nb_n$ with the $a_i \in I$ and $b_i \in J$ if and only if $\sigma(x) = \sigma(a_1)\sigma(b_1) + \cdots + \sigma(a_n)\sigma(b_n)$. It follows that $\sigma(IJ) = \sigma(I)\sigma(J)$. The action of G thus commutes with the group operation in $\mathcal{I}_B$.

If $I = \prod_i \mathfrak{q}_i^{e_i}$ is the unique factorization $I \in \mathcal{I}_B$, then $\sigma(I) = \prod_i \sigma(\mathfrak{q}_i)^{e_i}$ is the unique factorization of $\sigma(I)$. In particular, if $\mathfrak{q}$ is a prime of B the unique factorization of $\sigma(\mathfrak{q})$ is just $\sigma(\mathfrak{q})$, hence $\sigma(\mathfrak{q})$ is also a prime of B. □

Corollary 7.2. *Assume AKLBG, and let $\mathfrak{p}$ be a nonzero prime of A. Then G acts transitively on the set $\{\mathfrak{q}|\mathfrak{p}\}$ of primes $\mathfrak{q}$ of B that lie above $\mathfrak{p}$.*

Proof. Let $\sigma \in G$. For $\mathfrak{q}|\mathfrak{p}$ we have $\mathfrak{p}B \subseteq \mathfrak{q}$ and $\sigma(\mathfrak{p}B) \subseteq \sigma(\mathfrak{q})$, thus $\sigma(\mathfrak{q})|\mathfrak{p}$ and G acts on the set $\{\mathfrak{q}|\mathfrak{p}\}$. To show the action is transitive, let $\mathfrak{q}_1$ and $\mathfrak{q}_1$ be two primes lying above $\mathfrak{p}$, and suppose for the sake of contradiction that $\sigma(\mathfrak{q}) \neq \mathfrak{q}$‘ for all $\sigma \in G$. Let $\{\mathfrak{q}|\mathfrak{p}\} = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$. The CRT gives a ring isomorphism

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

Lecture by Andrew Sutherland

and we may choose $b \in \mathfrak{q}$‘ such that $b \equiv 1 \bmod \sigma^{-1}(\mathfrak{q})$ for all $\sigma \in G$. Then

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

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

Corollary 7.3. *Assume AKLBG and let $\mathfrak{p}$ be a nonzero 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 $\sigma \in G$ we have $\sigma(B) = B$, so σ restricts to an isomorphism of B and for each $\mathfrak{q}|\mathfrak{p}$ induces an isomorphism

$$\sigma\colon B/\mathfrak{q} \xrightarrow{\sim} B/\sigma(\mathfrak{q}).$$

It follows that $f_{\mathfrak{q}} = f_{\sigma(\mathfrak{q})}$, and since G acts transitively on $\{\mathfrak{q}|\mathfrak{p}\}$, all the $f_{\mathfrak{q}}$ must be equal.

For each $\sigma \in G$ we also have $\sigma(\mathfrak{p}) = \mathfrak{p}$ (since $\mathfrak{p} \subseteq A \subseteq K$) and $\sigma(B) = B$, so $\sigma(\mathfrak{p}B) = \mathfrak{p}B$. For each $\mathfrak{q}|\mathfrak{p}$ we have

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

and since G acts transitively on $\{\mathfrak{q}|\mathfrak{p}\}$ all the $e_{\mathfrak{q}}$ must be equal. □

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 $f_{\mathfrak{q}}$. We also define $g_{\mathfrak{p}} = \#\{\mathfrak{q}|\mathfrak{p}\}$.

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 5.31 and Corollary 7.3. □

Example 7.5. Assume *AKLBG*. When $n := [L\!:\!K]$ is prime there are just three possibilities for the factorization of each prime $\mathfrak{p}$ of A:

- $e_{\mathfrak{p}} = n$ 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 nonzero 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 nonzero prime of A. The decomposition groups $D_{\mathfrak{q}}$ for $\mathfrak{q}|\mathfrak{p}$ are all conjugate and have order $e_{\mathfrak{p}} f_{\mathfrak{p}}$ and index $g_{\mathfrak{p}}$ in G.*

Proof. For any group action, points in the same orbit have conjugate stabilizers. The stabilizers $D_{\mathfrak{q}}$ are all conjugate because the primes $\mathfrak{q}|\mathfrak{p}$ all lie in the same orbit (by Corollary 7.2). By the orbit stabilizer theorem, $[G : D_{\mathfrak{q}}] = \#\{\mathfrak{q}|\mathfrak{p}\} = g_{\mathfrak{p}}$, and since $|G| = [L : K] = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}$, we have $|D_{\mathfrak{q}}| = |G|/[G : D_{\mathfrak{q}}] = e_{\mathfrak{p}} f_{\mathfrak{p}}$. □

Let us now fix a prime $\mathfrak{q}$ of B lying above $\mathfrak{p} = \mathfrak{q} \cap A$. For each $\sigma \in G$ we have $\sigma(B) = B$, and if $\sigma \in D_\mathfrak{q}$ then we also have $\sigma(\mathfrak{q}) = \mathfrak{q}$, in which case σ induces a field automorphism $\overline{\sigma}$ of the residue field $B/\mathfrak{q}$. Since σ fixes $\mathfrak{p} \subseteq A \subseteq K$, the automorphism $\overline{\sigma}$ fixes the subfield $A/\mathfrak{p}$ of $B/\mathfrak{q}$. The map $\sigma \mapsto \overline{\sigma}$ defines a group homomorphism $\pi_\mathfrak{q} \colon D_\mathfrak{q} \to \operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q})$: it clearly preserves the identity, and for any $a \in B$ with image $\bar{a}$ in $B/\mathfrak{q}$ we have

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

In order to lighten the notation, we may use $\kappa(\mathfrak{p}) := A/\mathfrak{p}$ and $\kappa(\mathfrak{q}) := B/\mathfrak{q}$ to denote the residue fields of $\mathfrak{p}$ and $\mathfrak{q}$, respectively.

Proposition 7.8. *Assume AKLBG. Let $\mathfrak{q}$ be a prime of B lying above $\mathfrak{p} = A \cap \mathfrak{q}$. The residue field extension $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ is normal and the homomorphism $\pi_\mathfrak{q} \colon D_\mathfrak{q} \to \operatorname{Aut}_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{q}))$ defined by $\pi_\mathfrak{q}(\sigma) = \overline{\sigma}$ is surjective.*

Proof. Let F be the separable closure of $\kappa(\mathfrak{p})$ in $\kappa(\mathfrak{q})$, so that restriction to F induces an isomorphism $\operatorname{Aut}_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{q})) \xrightarrow{\sim} \operatorname{Gal}(F/\kappa(\mathfrak{p}))$. Since F is a finite separable extension of $\kappa(\mathfrak{p})$, it is simple, generated by some $\alpha \in F^\times$. Let us now pick $a \in B$ such that $a \equiv \alpha \bmod \mathfrak{q}$ and $a \equiv 0 \bmod \sigma^{-1}(\mathfrak{q})$ for all $\sigma \in G - D_\mathfrak{q}$; such an a exists by the CRT. Now define

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

and let $\overline{g}$ denote the image of g in $\kappa(\mathfrak{p})[x]$. For each $\sigma \in G - D_\mathfrak{q}$ the image of $\sigma(a)$ in $B/\mathfrak{q} = \kappa(\mathfrak{q})$ is 0 (by construction), so 0 is a root of $\overline{g}$ with multiplicity $m = \#(G - D_\mathfrak{q})$. The remaining roots are $\overline{\sigma}(\alpha)$ for $\sigma \in D_\mathfrak{q}$, which are all Galois conjugates of α. It follows that $\overline{g}(x)/x^m$ divides the minimal polynomial of α, but the minimal polynomial of α is irreducible in $\kappa(\mathfrak{p})[x]$, so $\overline{g}(x)/x^m$ *is* the minimal polynomial of α, and every conjugate of α is of the form $\overline{\sigma}(\alpha)$ for some $\sigma \in D_\mathfrak{q}$. Thus $D_\mathfrak{q}$ surjects onto $\operatorname{Gal}(F/\kappa(\mathfrak{p})) \simeq \operatorname{Aut}_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{q}))$ and $\pi_\mathfrak{q}$ is surjective.

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

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

Corollary 7.10. *Assume AKLBG and let $\mathfrak{q}$ be a prime of B lying above $\mathfrak{p} = A \cap \mathfrak{q}$. We have an exact sequence of groups*

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

and $|I_\mathfrak{q}| = e_\mathfrak{p}[\kappa(\mathfrak{q}) : \kappa(\mathfrak{p})]_i$.

For the sake of convenience, let us now assume that $\kappa(\mathfrak{q})$ is a separable extension of $\kappa(\mathfrak{p})$; this holds, for example, whenever $\kappa(\mathfrak{p})$ is finite, which includes the main case we care about, in which K is a global field (a number field or a function field). Under this assumption $\kappa(\mathfrak{q})$ is a Galois extension of $\kappa(\mathfrak{p})$, and we have

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

Proposition 7.11. *Assume AKLBG, let $\mathfrak{q}$ be a prime of B lying above $\mathfrak{p} = A \cap \mathfrak{q}$, and assume that $\kappa(\mathfrak{q}) := B/\mathfrak{q}$ is a separable extension of $\kappa(\mathfrak{p}) := A/\mathfrak{p}$. We then have the tower of field extensions $K \subseteq L^{D_\mathfrak{q}} \subseteq L^{I_\mathfrak{q}} \subseteq L$ with degrees*

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

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 statement follows immediately from Lemma 7.7 and $[L : K] = e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p}$. The second follows from Proposition 7.8 and the assumption that $\kappa(\mathfrak{q})/\kappa(/\mathfrak{p})$ is separable, since $D_\mathfrak{q}/I_\mathfrak{q} \simeq \operatorname{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ has cardinality $f_\mathfrak{p} = [\kappa(\mathfrak{q}) : \kappa(\mathfrak{p})]$. Then $[L : L^{D_\mathfrak{q}}] = |D_\mathfrak{q}| = e_\mathfrak{p} f_\mathfrak{p}$ and $|D_\mathfrak{q}| = |I_\mathfrak{q}| \cdot |D_\mathfrak{q}/I_\mathfrak{q}|$ imply the third. □

We now consider an intermediate field E lying between K and L. Let us fix a prime $\mathfrak{q}$ of B lying above $\mathfrak{p} := \mathfrak{q} \cap K$, and let $\mathfrak{q}_E := \mathfrak{q} \cap E$, so that $\mathfrak{q}|\mathfrak{q}_E$ and $\mathfrak{q}_E|\mathfrak{p}$. Let $\kappa(\mathfrak{p})$, $\kappa(\mathfrak{q}_E)$, $\kappa(\mathfrak{q})$ be the residue fields of $\mathfrak{p}$, $\mathfrak{q}_E$, $\mathfrak{q}$, respectively, and define $\overline{G}_\mathfrak{q}(L/K) := \operatorname{Aut}_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{q}))$, $\overline{G}_\mathfrak{q}(L/E) := \operatorname{Aut}_{\kappa(\mathfrak{q}_E)}(\kappa(\mathfrak{q}))$, $\overline{G}_{\mathfrak{q}_E}(E/K) := \operatorname{Aut}_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{q}_E))$.

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

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

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 $D_\mathfrak{q}(L/E) \subseteq \operatorname{Gal}(L/E) \subseteq \operatorname{Gal}(L/K)$. An element σ of $\operatorname{Gal}(L/K)$ lies in $D_\mathfrak{q}(L/E)$ if and only if it fixes E (hence lies in $\operatorname{Gal}(L/E)$) and satisfies $\sigma(\mathfrak{q}) = \mathfrak{q}$ (hence lies in $D_\mathfrak{q}(L/K)$). 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 precisely 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 $\operatorname{Gal}(L/E)$.

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 as 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 $\operatorname{Hom}_K(L,\Omega) \to \operatorname{Hom}_E(L,\Omega) \times \operatorname{Hom}_K(E,\Omega)$ whose second factor is restriction, and we may view this as a bijection $\phi\colon \operatorname{Gal}(L,K) \to \operatorname{Gal}(L/E) \times \operatorname{Gal}(E/K)$. If $\sigma \in \operatorname{Gal}(E/K)$ stabilizes $\mathfrak{q}_E$ then $\phi^{-1}(1,\sigma) \in \operatorname{Gal}(L/K)$ 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 (this implies commutativity of the whole 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 $D_{\mathfrak{q}}(L/E)$. In the lower right square 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 (if any are finite, they all must be). 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 $A/\mathfrak{p}$: finite fields are perfect, so the extension is separable, and we proved in the previous lecture that the residue field extension is always normal (whether the residue fields are separable/finite or not); see Proposition 7.8.

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 $\mathbb{F}_{\mathfrak{q}}$). There are two distinct possibilities, depending on the characteristic of K. If K has characteristic 0 (as when K is a number field), its characteristic differs from the residue field characteristic, which may vary with $\mathfrak{p}$ but is necessarily nonzero because $A/\mathfrak{p}$ is finite; this is as a *mixed characteristic* setting. If K has positive characteristic p (as when K is a global function field), the residue fields necessarily have the same characteristic (the ring homomorphism $A \to A/\mathfrak{p}$ sends 1 to 1, and if $1 + \cdots + 1 = 0$ in $A \subseteq K$, the same holds in $A/\mathfrak{p}$); this is an *equal characteristic* setting.

Let $\mathfrak{p}$ be a prime of K and let $\mathfrak{q}|\mathfrak{p}$ be a prime of L lying above $\mathfrak{p}$. Corollary 7.10 gives us an exact sequence

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

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

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

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

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

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.

Definition 7.13. Assume *AKLBG* with finite residue fields and $\mathfrak{q}|\mathfrak{p}$ unramified. The inverse image of the Frobenius automorphism of $\operatorname{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$ under $\pi_{\mathfrak{q}} : D_{\mathfrak{q}} \xrightarrow{\sim} \operatorname{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$ is the *Frobenius element* $\sigma_{\mathfrak{q}} \in D_{\mathfrak{q}} \subseteq G$ (also called the *Frobenius substitution* [1, §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 $\sigma(x) \equiv x^{\#\mathbb{F}_\mathfrak{p}} \equiv 0^{\#\mathbb{F}_\mathfrak{p}} \equiv 0 \bmod \mathfrak{q}$, thus $\sigma(x) \in \mathfrak{q}$; it follows that $\sigma(\mathfrak{q}) = \mathfrak{q}$, and therefore $\sigma \in D_\mathfrak{q}$. The isomorphism $\pi_\mathfrak{q} \colon D_\mathfrak{q} \to \operatorname{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ maps both σ and $\sigma_\mathfrak{q}$ to the Frobenius automorphism $x \mapsto x^{\#\mathbb{F}_\mathfrak{p}}$, hence they must be equal. □

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 $\operatorname{Frob}_\mathfrak{p}$.

It is common to abuse terminology and refer to $\operatorname{Frob}_\mathfrak{p}$ 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 $\operatorname{Frob}_\mathfrak{p} = \{\sigma_\mathfrak{q} : \mathfrak{q}|\mathfrak{p}\}$ is a singleton set and there is a unique choice for $\sigma_\mathfrak{p}$.

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 $\mathfrak{q}_E \coloneqq \mathfrak{q} \cap E$. 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 $\mathrm{Gal}(\mathbb{F}_{\mathfrak{q}_E}/\mathbb{F}_{\mathfrak{p}})$ is the restriction of the Frobenius automorphism $x \mapsto x^{\#\mathbb{F}_{\mathfrak{p}}}$ of $\mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$ 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

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

where $\mathfrak{q}$ is any primve 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 $G = \mathrm{Gal}(L/K)$, but ramified primes $\mathfrak{q}|\mathfrak{p}$ cause problems: the homomorphism $\pi_{\mathfrak{q}}\colon D_{\mathfrak{q}} \to \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_{\mathfrak{p}})$ 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.

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

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

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 $\mathrm{Gal}(L/K)$ 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 $p \not| D$ 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] J.-P. Serre, *Local fields*, Springer, 1979.

18.785 Number Theory I
Fall 2016