# 7 Orders in Dedekind domains, primes in Galois extensions

## 7.1 Orders in Dedekind domains

Let $S/R$ be an extension of rings. The *conductor* $\mathfrak{c}$ of $R$ (in $S$) is the largest $S$-ideal that is also an $R$-ideal, equivalently,

$$\mathfrak{c} := \{r \in R : rS \subseteq R\}.$$

This definition applies to any ring extension, but we are interested in the case where $R$ is a noetherian domain and $S$ is the integral closure of $R$. Thus whenever we speak of the conductor of a domain $R$, we always mean the conductor of $R$ in its integral closure $S$. In this situation the conductor is nonzero precisely when $S$ is finite over $R$.

**Lemma 7.1.** *Let $R$ be a noetherian domain. The conductor of $R$ in its integral closure $S$ is nonzero if and only if $S$ is finitely generated as an $R$-module.*

*Proof.* This is a special case of Lemma 3.3. □

We now introduce the notion of an *order* (in a Dedekind domain).

**Definition 7.2.** An *order* $\mathcal{O}$ is a noetherian domain of dimension one whose conductor is nonzero, equivalently, whose integral closure is finitely generated as an $\mathcal{O}$-module.[1]

Note that the integral closure of an order is a Dedekind domain. As shown by Nagata [1, p. 212], noetherian domains of dimension one with zero conductor do exist, but in the cases of interest to us the requirement the conductor be nonzero is automatically satisifed.

**Example 7.3.** In the $AKLB$ setting, where $B$ is the integral closure of $A$ in a finite separable extension $L$ of the fraction field $K$ of $A$, if we write $L = K(\alpha)$ with $\alpha \in B$, then $\mathcal{O} = A[\alpha]$ is an order with fraction field $L$. Its conductor is nonzero because $B$ is finitely generated over $A$ (by Proposition 4.60), hence over $A[\alpha]$.

**Remark 7.4.** There is a more general notion of an order than the one we have given here. Let $A$ be a noetherian domain with fraction field $K$, and let $L$ be a (not necessarily commutative) $K$-algebra of finite dimension. An $A$-*order* in $L$ is a subring $\mathcal{O}$ of $L$ that is also an $A$-lattice (finitely generated $A$-submodule of $L$ that spans $L$ as a $K$-vector space). In the $AKLB$-setting, any order $\mathcal{O}$ with integral closure $B$ is also an $A$-order in $L$, and if we assume that $A$ has dimension one, commutative $A$-orders are orders under our definition above. But in general the $K$-algebra $L$ and the order $\mathcal{O}$ need not be commutative. For example, the endomorphism ring of an elliptic curve $E/k$ (where $k$ is any field) is isomorphic to a $\mathbb{Z}$-order $\mathcal{O}$ in a $\mathbb{Q}$-algebra $L$ of dimension 1, 2, or 4. The $\mathbb{Z}$-order $\mathcal{O}$ is commutative in the dimension 1 and 2 cases, where $L$ is either $\mathbb{Q}$ or an imaginary quadratic field, but it is non-commutative in the dimension 4 case, where $L$ is a quaternion algebra.

As with Dedekind domains, by a prime $\mathfrak{p}$ of an order $\mathcal{O}$ we mean a nonzero (hence maximal) prime $\mathcal{O}$-ideal, and if $\mathfrak{q}$ is a prime of the integral closure $B$ of $\mathcal{O}$ lying above $\mathfrak{p}$ (dividing $\mathfrak{p}B$) then we may write $\mathfrak{q}|\mathfrak{p}$ to indicate this. As in the $AKLB$ setup, we have $\mathfrak{q}|\mathfrak{p}$ if and only if $\mathfrak{q} \cap \mathcal{O} = \mathfrak{p}$ (see Lemma 5.1).

[1] Not all authors require an order to have nonzero conductor (e.g. Neukirch [2, §I.12]), but most of the interesting theorems about orders require this assumption.

**Lemma 7.5.** *Let $\mathcal{O}$ be an order with integral closure $B$ and conductor $\mathfrak{c}$. A prime $\mathfrak{q}$ of $B$ contains $\mathfrak{c}$ if and only if the prime $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}$ of $\mathcal{O}$ contains $\mathfrak{c}$. In particular, only finitely many primes $\mathfrak{p}$ of $\mathcal{O}$ contain $\mathfrak{c}$.*

*Proof.* Let $\mathfrak{q}$ be a prime of $B$. We have $\mathfrak{c} \subseteq \mathcal{O}$, thus $\mathfrak{q}$ contains $\mathfrak{c}$ if and only if $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}$ contains $\mathfrak{c}$. The factorization of the ideal $\mathfrak{c}$ in $B$ includes only many prime ideals $\mathfrak{q}$, and each such $\mathfrak{q}$ lies above only one prime $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}$ of $\mathcal{O}$. □

**Lemma 7.6.** *Let $\mathcal{O}$ be an order with integral closure $B$ and conductor $\mathfrak{c}$. Let $\mathfrak{p}$ be a prime of $\mathcal{O}$ that does not contain $\mathfrak{c}$. Then $\mathfrak{p}B$ is a prime of $B$.*

*Proof.* Fix $s \in \mathfrak{c} - \mathfrak{p}$. We claim that for any prime $\mathfrak{q}|\mathfrak{p}$ we have $\mathcal{O}_\mathfrak{p} = B_\mathfrak{q}$. Certainly $\mathcal{O}_\mathfrak{p} \subseteq B_\mathfrak{q}$: for any $x = a/d \in \mathcal{O}_p$ with $a \in \mathcal{O}$ and $d \in \mathcal{O} - \mathfrak{p}$ we have $a \in B$ and $d \notin (B - \mathfrak{q}) \cap \mathcal{O} = B - \mathfrak{q}$. Conversely, for any $b/t \in B_\mathfrak{q}$ with $b \in B$ and $t \in B - \mathfrak{q}$, we have $b/t = (sb)/(st) \in \mathcal{O}_\mathfrak{p}$, since $sb \in \mathcal{O}$ and $st \in \mathcal{O} - \mathfrak{p}$ (note $s \notin \mathfrak{p} \subseteq \mathfrak{q}$ and $t \notin \mathfrak{q}$, so $st \notin \mathfrak{q} \supseteq \mathfrak{p}$), thus $B_\mathfrak{q} \subseteq \mathcal{O}_p$.

It follows that there is a unique prime $\mathfrak{q}$ of $B$ lying above $\mathfrak{p}$ (since $B_\mathfrak{q} \neq B_{\mathfrak{q}'}$ if $\mathfrak{q} \neq \mathfrak{q}'$). We thus have $\mathfrak{p}B = \mathfrak{q}^e$ for some $e \geq 1$, and we claim that $e = 1$. Indeed, we must have $\mathfrak{p}\mathcal{O}_\mathfrak{p} = \mathfrak{q}B_\mathfrak{q}$ (this is the unique maximal ideal of the local ring $\mathcal{O}_\mathfrak{p} = B_\mathfrak{q}$ written in two different ways), so $\mathfrak{q}^e B_\mathfrak{q} = \mathfrak{q}B_\mathfrak{q}$ and therefore $e = 1$. □

**Corollary 7.7.** *Let $\mathcal{O}$ be an order with integral closure $B$ and conductor $\mathfrak{c}$. The restriction of the map $\operatorname{Spec} B \to \operatorname{Spec} \mathcal{O}$ defined by $\mathfrak{q} \mapsto \mathfrak{q} \cap \mathcal{O}$ to prime ideals that do not contain $\mathfrak{c}$ is a bijection with inverse $\mathfrak{p} \mapsto \mathfrak{p}B$.*

**Theorem 7.8.** *Let $\mathcal{O}$ be an order with integral closure $B$ and conductor $\mathfrak{c}$, and let $\mathfrak{p}$ be a prime of $\mathcal{O}$. The following are equivalent:*

(a) *$\mathfrak{p}$ does not contain $\mathfrak{c}$;*

(b) *$\mathcal{O} = \{x \in B : x\mathfrak{p} \subseteq \mathfrak{p}\}$;*

(c) *$\mathfrak{p}$ is invertible;*

(d) *$\mathcal{O}_\mathfrak{p}$ is a DVR;*

(e) *$\mathfrak{p}\mathcal{O}_\mathfrak{p}$ is principal.*

*If any of these equivalent properties hold, then $\mathfrak{p}B$ is a prime of $B$.*

*Proof.* See Problem Set 4. □

Recall that two ideals $I$ and $J$ in a ring $A$ are said to be *relatively prime* if $I + J = A$; we may also say that $I$ is *prime to $J$*. It follows from the localization results we proved in Lectures 2 and 3 that, at least when $A$ is a noetherian domain, this is equivalent to requiring that $I_\mathfrak{p} + J_\mathfrak{p} = A_\mathfrak{p}$ for every prime ideal $\mathfrak{p}$ of $A$. For prime ideals $\mathfrak{p}$ that do not contain $J$, we have $J_\mathfrak{p} = A_\mathfrak{p}$, in which case this condition is trivially satisfied. On the other hand, if $\mathfrak{p}$ contains $J$, then $J_\mathfrak{p}$ is contained in the unique maximal ideal $\mathfrak{p}A_\mathfrak{p}$ of the local ring $A_\mathfrak{p}$, and we can have $I_\mathfrak{p} + J_\mathfrak{p} = A_\mathfrak{p}$ only when $I_\mathfrak{p} \not\subseteq \mathfrak{p}A_\mathfrak{p}$, in which case $I_\mathfrak{p} = A_\mathfrak{p}$. This leads to the following definition.

**Definition 7.9.** Let $A$ be a noetherian domain and let $J$ be and ideal of $A$. A fractional ideal $I$ of $A$ is *prime to $J$* if $IA_\mathfrak{p} = A_\mathfrak{p}$ for all prime ideals $\mathfrak{p}$ that contain $J$.

**Corollary 7.10.** *Let $\mathcal{O}$ be an order with integral closure $B$ and conductor $\mathfrak{c}$, and let $\mathcal{I}_{\mathcal{O}}^{\mathfrak{c}}$ and $\mathcal{I}_B^{\mathfrak{c}}$ denote the sets of fractional ideals of $\mathcal{O}$ and $B$, respectively, that are prime to the conductor $\mathfrak{c}$. The map $\mathfrak{q} \mapsto \mathfrak{q} \cap \mathcal{O}$ induces a group isomorphism from $\mathcal{I}_B^{\mathfrak{c}}$ to $\mathcal{I}_{\mathcal{O}}^{\mathfrak{c}}$. In particular, every fractional ideal in $I_{\mathcal{O}}^{\mathfrak{c}}$ can be uniquely factored into prime ideals that do not contain $\mathfrak{c}$.*

**Remark 7.11.** Orders in Dedekind domains also have a geometric interpretation. If $\mathcal{O}$ is an order, the curve $X = \operatorname{Spec} \mathcal{O}$ will have a singularity at each closed point $P$ corresponding to a maximal ideal of $\mathcal{O}$ that contains the conductor. Taking the integral closure $B$ of $\mathcal{O}$ yields a smooth curve $Y = \operatorname{Spec} B$ with the same function field as $X$ and a morphism $Y \to X$ that looks like a bijection above non-singular points (a dominant morphism of degree 1). The curve $Y$ is called the *normalization* of $X$.

## 7.2 Splitting primes in Galois extensions

We now return to our standard $AKLB$ setup: $A$ is a Dedekind domain with $K$ as its fraction field, $L$ is a finite separable extension of $K$, and $B$ is the integral closure of $A$ in $L$ (so $B$ is a Dedekind domain with fraction field $L$). We now add the additional hypothesis that $L/K$ is a normal extension, equivalently, $L/K$ is Galois, and let $G := \operatorname{Gal}(L/K)$ denote the Galois group. We will use the shorthand $AKLBG$ to denote this setup. Recall that by a *prime* of $A$ (or $K$) we mean a nonzero prime ideal of $A$, and similarly for $B$ (or $L$).

**Theorem 7.12.** *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 $A$ and therefore the root of some monic polynomial $f \in A[x] \subset K[x]$ whose coefficients are fixed by $\sigma$. 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 $\sigma$ is a field automorphism, and if $a \in I$ and $b \in B$ then $\sigma^{-1}(b)a \in I$, since $\sigma^{-1}(b) \in B$ and $I$ is a $B$-ideal, 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 $\sigma \in G$ acts on 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 $\mathcal{I}_B$.

For any $I, J \in \mathcal{I}_B$ and $\sigma \in G$, if $x = a_1 b_1 + \cdots + a_n b_n$ with the $a_i \in I$ and $b_i \in J$, then $\sigma(x) = \sigma(a_1)\sigma(b_1) + \cdots + \sigma(a_n)\sigma(b_n)$ and therefore $\sigma(IJ) \subseteq \sigma(I)\sigma(J)$. Conversely, if $y = \sigma(a_1)\sigma(b_1) + \cdots + \sigma(a_n)\sigma(b_n)$ then $y = \sigma(a_1 b_1 + \cdots + a_n b_n) \in \sigma(IJ)$ so $\sigma(I)\sigma(J) \subseteq \sigma(IJ)$ and $\sigma(IJ) = \sigma(I)\sigma(J)$. The action of $G$ thus commutes with the group operation in $\mathcal{I}_B$.

It follows that if $I = \prod_i \mathfrak{q}_i^{e_i}$ is the unique factorization of a fractional ideal $I$ of $B$, 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 nonzero prime ideal of $B$ then the unique factorization of $\sigma(\mathfrak{q})$ is just $\sigma(\mathfrak{q})$, hence $\sigma(\mathfrak{q})$ is prime. $\square$

**Corollary 7.13.** *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 any prime $\mathfrak{q}|\mathfrak{p}$ we have $\mathfrak{p}B \subseteq \mathfrak{q}$, thus $\sigma(\mathfrak{p}B) \subseteq \sigma(\mathfrak{q})$, so $\sigma(\mathfrak{q})|\mathfrak{p}$, and it follows from the theorem that $G$ acts on the set $\{\mathfrak{q}|\mathfrak{p}\}$.

To show the action is transitive, let $\mathfrak{q}$ and $\mathfrak{q}'$ be two primes lying above $\mathfrak{p}$, and suppose for the sake of contradiction that $\sigma(\mathfrak{q}) \neq \mathfrak{q}'$ for all $\sigma \in G$. By the Chinese remainder theorem, 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 7.14.** *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 $\sigma$ 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 $\mathfrak{q}|\mathfrak{p}$ we also have

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

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 7.15.** *Assume AKLBG and let $n = [L : K]$. For each nonzero prime $\mathfrak{p}$ of $A$ we have $n = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}$.*

**Example 7.16.** 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.

## 7.3 Decomposition and inertia groups

**Definition 7.17.** 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 7.18.** *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 $G_{\mathfrak{q}} = D_{\mathfrak{q}}$ are all conjugate because the primes $\mathfrak{q}|\mathfrak{p}$ all lie in the same orbit (by Corollary 7.13). 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 $\sigma(\mathfrak{q}) = \mathfrak{q}$ and $\sigma$ induces a field automorphism $\overline{\sigma}$ of the residue field $B/\mathfrak{q}$. Since $\sigma$ fixes $\mathfrak{p} \subseteq A \subseteq K$, the automorphism $\overline{\sigma}$ fixes the subfield $A/\mathfrak{p}$ of $B/\mathfrak{q}$. This gives us a map $\sigma \mapsto \overline{\sigma}$ from $D_{\mathfrak{q}}$ to $\operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q})$.

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 and $\mathfrak{p}$ and $\mathfrak{q}$, respectively.

**Proposition 7.19.** *Assume AKLBG. Let $\mathfrak{q}$ be a prime of $B$ lying above $\mathfrak{p} = A \cap \mathfrak{q}$. The residue field $\kappa(\mathfrak{q}) := B/\mathfrak{q}$ is a normal extension of $\kappa(\mathfrak{p}) := A/\mathfrak{p}$, and the map*

$$\begin{aligned} \pi_{\mathfrak{q}} \colon D_{\mathfrak{q}} &\to \operatorname{Aut}_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{q})) \\ \sigma &\mapsto \overline{\sigma} \end{aligned}$$

*defined above is a surjective group homomorphism.*

*Proof.* The map $\pi_{\mathfrak{q}}$ clearly preserves the identity element, and for any $\sigma, \tau \in D_{\mathfrak{q}}$ we have $\overline{\sigma\tau} = \overline{\sigma}\,\overline{\tau}$ because the action of $D_{\mathfrak{q}}$ on $B$ fixes $\mathfrak{q}$ and commutes with quotienting by $\mathfrak{q}$.

To show surjectivity, let $F$ be the separable closure of $\kappa(\mathfrak{p})$ in $\kappa(\mathfrak{q})$, so that restriction to $F$ induces an isomorphism from $\operatorname{Aut}_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{q}))$ to $\operatorname{Gal}(F/\kappa(\mathfrak{p}))$. 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 Chinese remainder theorem. 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 $\kappa(\mathfrak{p})[x]$. 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 $\alpha$. It follows that $\overline{g}(x)/x^m$ divides the minimal polynomial of $\alpha$, but the minimal polynomial of $\alpha$ is irreducible in $\kappa(\mathfrak{p})[x]$, so $\overline{g}(x)/x^m$ *is* the minimal polynomial of $\alpha$, and every conjugate of $\alpha$ is of the form $\overline{\sigma}(\alpha)$ for some $\sigma \in D_{\mathfrak{q}}$. Thus $D_{\mathfrak{q}}$ surjects onto $\operatorname{Gal}(F/\kappa(\mathfrak{p})) \simeq \operatorname{Aut}_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{q}))$, so $\pi_{\mathfrak{q}}$ 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 7.20.** 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 7.21.** *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, where $K$ 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 7.22.** *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 fixed fields $L^{D_{\mathfrak{q}}}$ and $L^{I_{\mathfrak{q}}}$ in the proposition are the *decomposition field* and the *inertia field* associated to $\mathfrak{q}$.

*Proof.* The third statement follows immediately from Lemma 7.18 and $[L : K] = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}$. The second follows from Proposition 7.19 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 nonzero prime $\mathfrak{q}$ of $B$ lying above the prime $\mathfrak{p} = \mathfrak{q} \cap K$, and let $\mathfrak{q}_E = \mathfrak{q} \cap E$, so that $\mathfrak{q}|\mathfrak{q}_E$ and $\mathfrak{q}_E|\mathfrak{p}$.

To simplify the notation we use $\kappa(\mathfrak{p})$, $\kappa(\mathfrak{q}_E)$, and $\kappa(\mathfrak{q})$ to denote the residue fields of $\mathfrak{p}$, $\mathfrak{q}_E$, and $\mathfrak{q}$ as above, and define $\overline{G}_{\mathfrak{q}}(L/K) := \operatorname{Aut}_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{q}))$ and similarly define the automorphism groups $\overline{G}(L/E)$ and $\overline{G}(E/K)$.

**Proposition 7.23.** *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.* For the first claim, each $\sigma \in D_{\mathfrak{q}}(L/E)$ lies in $\operatorname{Gal}(L/E) \subseteq \operatorname{Gal}(L/K)$ and stabilizes $\mathfrak{q}$ as an element of $\{\mathfrak{q}|\mathfrak{q}_E\}$, but $\mathfrak{q}_E \subseteq E$, so $\sigma$ stabilizes $\mathfrak{q}$ as an element of $\{\mathfrak{q}|\mathfrak{p}\}$ and lies in $D_{\mathfrak{q}}(L/K)$. Conversely, each $\sigma \in D_{\mathfrak{q}}(L/K) \cap \operatorname{Gal}(L/E)$ stabilizes $\mathfrak{q}$ as an element of $\{\mathfrak{q}|\mathfrak{p}\}$ and fixes $E \supseteq \mathfrak{q}_E$ and therefore is an element of $\operatorname{Gal}(L/E)$ that stabilizes $\mathfrak{q}$ as an element of $\{\mathfrak{q}|\mathfrak{q}_E\}$, hence an element of $D_{\mathfrak{q}}(L/E)$. For the second claim, the restriction of the map $\pi_{\mathfrak{q}}\colon D_{\mathfrak{q}}(L/K) \to \overline{G}_{\mathfrak{q}}(L/K)$ to $D_{\mathfrak{q}}(L/E)$ is precisely the map $\pi_{\mathfrak{q}}\colon D_{\mathfrak{q}}(L/E) \to \overline{G}_{\mathfrak{q}}(L/E)$, hence the kernels agree after intersecting with $\operatorname{Gal}(L/E)$.

The exactness of the three columns follows immediately from Corollary 7.21. We now argue exactness of the first two rows. In both cases the rows correspond to an inclusion of automorphisms of $L$ that fix $E$ (and hence fix $K$), followed by restriction to $E$. Injectivity of the inclusion map is clear, and exactness at the middle term is also clear (the automorphisms of $L$ that restrict to the trivial automorphism on $E$ are precisely the ones that fix $E$). Surjectivity of the restriction map follows from the fact that we can extend any automorphism of $E$ to an automorphism of $L$, since $L/E$ is an algebraic extension (indeed, $L = E(\alpha)$ for some $\alpha$ that we can leave fixed, since $L/E$ is finite separable).

For the bottom row we have the tower of residue fields $\kappa(\mathfrak{p}) \subseteq \kappa(\mathfrak{q}_E) \subseteq \kappa(\mathfrak{q})$, and get an exact sequence as follows: $\overline{G}(L/E)$ is included in $\overline{G}(L/K)$ which surjects onto $\overline{G}(E/K)$ via restriction, and the elements of $\overline{G}(L/K)$ whose restriction is the identity are precisely the elements of $\overline{G}(L/E)$ (this is just standard Galois theory, it applies to any tower $F_1 \subseteq F_2 \subseteq F_3$ with $F_3/F_1$ and $F_2/F_1$ both normal).

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 $D_{\mathfrak{q}_E}(L/E)$. The lower right square the horizontal maps are restrictions and the vertical maps agree after restriction to $E$. □

## References

[1] M. Nagata, *Local rings*, John Wiley & Sons, 1962.

[2] J. Neukirch, *Algebraic number theory*, Springer, 1999.