Chapter 2.
Valuations and Linear Disjointness

Sections 2.1–2.4 introduce the basic elements of the theory of valuations, especially discrete valuations, and of Dedekind domains. These sections are primarily a survey. We prove that an overring of a Dedekind domain is again a Dedekind domain (Proposition 2.4.7).

The rest of the chapter centers around the notion of linear disjointness of fields. We use this notion to define separable, regular, and primary extensions of fields. In particular, we prove that an extension F/K with a K-rational place is regular. Section 2.8 gives a useful criterion for separability with derivatives.

2.1 Valuations, Places, and Valuation Rings

The literature treats arithmetic theory of fields through three intimately connected classes of objects: valuations, places, and valuation rings. We briefly review the basic definitions.

Call an Abelian (additive) group Γ with a binary relation $<$ an **ordered group** if the following statements hold for all $\alpha, \beta, \gamma \in \Gamma$.

(1a) Either $\alpha < \beta$, or $\alpha = \beta$, or $\beta < \alpha$.
(1b) If $\alpha < \beta$ and $\beta < \gamma$, then $\alpha < \gamma$.
(1c) If $\alpha < \beta$, then $\alpha + \gamma < \beta + \gamma$.

Some examples of ordered groups are the additive groups $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{Z} \oplus \mathbb{Z}$ with the order $(m, n) < (m', n')$ if either $m < m'$ or $m = m'$ and $n < n'$ (the **lexicographic order**).

A **valuation** v of a field F is a map of F into a set $\Gamma \cup \{\infty\}$, where Γ is an ordered group, with these properties:

(2a) $v(ab) = v(a) + v(b)$.
(2b) $v(a + b) \geq \min\big(v(a), v(b)\big)$.
(2c) $v(a) = \infty$ if and only if $a = 0$.
(2d) There exists $a \in F^\times$ with $v(a) \neq 0$.

By definition the symbol ∞ satisfies these rules:

(3a) $\infty + \infty = \alpha + \infty = \infty + \alpha = \infty$; and
(3b) $\alpha < \infty$ for each $\alpha \in \Gamma$.

Condition (2) implies several more properties of v:

(4a) $v(1) = 0$, $v(-a) = v(a)$.
(4b) If $v(a) < v(b)$, then $v(a + b) = v(a)$ (Use the identity $a = (a + b) - b$ and (2b));
(4c) If $\sum_{i=1}^{n} a_i = 0$, then there exist $i \neq j$ such that $v(a_i) = v(a_j)$ and $v(a_i) = \min(v(a_1), \ldots, v(a_n))$ (Use (2b) and (4b)).

We refer to the pair (F, v) as a **valued field**.

The subgroup $\Gamma_v = v(F^\times)$ of Γ is the **value group** of v. The set $O_v = \{a \in F \mid v(a) \geq 0\}$ is the **valuation ring** of v. It has a unique maximal ideal $\mathfrak{m}_v = \{a \in F \mid v(a) > 0\}$. Refer to the residue field $\bar{F}_v = O_v/\mathfrak{m}_v$ as the **residue field** of F at v. Likewise, whenever there is no ambiguity, we denote the coset $a + \mathfrak{m}_v$ by $\bar{a}$ and call it the **residue** of a at v.

Two valuations v_1, v_2 of a field F with value groups Γ_1, Γ_2 are **equivalent** if there exists an isomorphism $f\colon \Gamma_1 \to \Gamma_2$ with $v_2 = f \circ v_1$. Starting from Section 2.2, we abuse our language and say that v_1 and v_2 are **distinct** if they are inequivalent.

A **place** of a field F is a map φ of F into a set $M \cup \{\infty\}$, where M is a field, with these properties:

(5a) $\varphi(a+b) = \varphi(a) + \varphi(b)$.

(5b) $\varphi(ab) = \varphi(a)\varphi(b)$.

(5c) There exist $a, b \in F$ with $\varphi(a) = \infty$ and $\varphi(b) \neq 0, \infty$.

By definition the symbol ∞ satisfies the following rules:

(6a) $x + \infty = \infty + x = \infty$ for each $x \in M$.

(6b) $x \cdot \infty = \infty \cdot x = \infty \cdot \infty = \infty$ for each $x \in M^\times$.

(6c) Neither $\infty + \infty$, nor $0 \cdot \infty$ are defined.

It is understood that (5a) and (5b) hold whenever the right hand side is defined. These conditions imply that $\varphi(1) = 1$, $\varphi(0) = 0$ and $\varphi(x^{-1}) = \varphi(x)^{-1}$. In particular, if $x \neq 0$, then $\varphi(x) = 0$ if and only if $\varphi(x^{-1}) = \infty$.

We call an element $x \in F$ with $\varphi(x) \neq \infty$ **finite** at φ, and say that φ is **finite** at x. The subring of all elements finite at φ, $O_\varphi = \{a \in F \mid \varphi(a) \neq \infty\}$, is the **valuation ring** of φ. It has a unique maximal ideal $\mathfrak{m}_\varphi = \{a \in F \mid \varphi(a) = 0\}$. The quotient ring $O_\varphi/\mathfrak{m}_\varphi$ is a field which is canonically isomorphic to the **residue field** $\bar{F}_\varphi = \{\varphi(a) \mid a \in O_\varphi\}$ of F at φ. The latter is a subfield of M. Call φ a **K-place** if K is a subfield of F and $\varphi(a) = a$ for each $a \in K$.

Two places φ_1 and φ_2 of a field F with residue fields M_1 and M_2 are **equivalent** if there exists an isomorphism $\lambda\colon M_1 \to M_2$ with $\varphi_2 = \lambda \circ \varphi_1$.

A **valuation ring** of a field F is a proper subring O of F such that if $x \in F^\times$, then $x \in O$ or $x^{-1} \in O$. The subset $\mathfrak{m} = \{x \in O \mid x^{-1} \notin O\}$ is the unique maximal ideal of O (Exercise 1). The map $\varphi\colon F \to O/\mathfrak{m} \cup \{\infty\}$ which maps $x \in O$ onto its residue class modulo $\mathfrak{m}$ and maps $x \in F \setminus O$ onto ∞ is a place of F with valuation ring O. Denote the units of O by $U = \{x \in O \mid x^{-1} \in O\}$. Then $F^\times/U$ is a multiplicative group ordered by the rule $xU \leq yU \iff yx^{-1} \in O$. The map $x \mapsto xU$ defines a valuation of F with O being its valuation ring.

These definitions easily give a bijective correspondence between the valuation classes, the place classes and the valuation rings of a field F.

An isomorphism $\sigma\colon F \to F'$ of fields induces a bijective map of the valuations and places of F onto those of F' according to the following rule: If v is a valuation of F, then $\sigma(v)$ is defined by $\sigma(v)(x) = v(\sigma^{-1}x)$ for every $x \in F'$. If φ is a place of F, then $\sigma(\varphi)(x) = \varphi(\sigma^{-1}x)$. In particular, σ

induces an isomorphism $\bar{F}_\varphi \cong \bar{F}'_{\sigma(\varphi)}$ of residue fields. It is also clear that if φ corresponds to v, then $\sigma(\varphi)$ corresponds to $\sigma(v)$.

A valuation v of a field F is **real** (or of **rank** 1) if Γ_v is isomorphic to a subgroup of $\mathbb{R}$. Real valuations satisfy the so called **weak approximation theorem**, a generalization of the Chinese remainder theorem [Cassels-Fröhlich, p. 48]:

PROPOSITION 2.1.1: *Consider the following objects: inequivalent real valuations $v_1, \ldots, v_n$ of a field F, elements $x_1, \ldots, x_n$ of F, and real numbers $\gamma_1, \ldots, \gamma_n$. Then there exists $x \in F$ with $v_i(x - x_i) \geq \gamma_i$, $i = 1, \ldots, n$.*

2.2 Discrete Valuations

A valuation v of a field F is **discrete** if $v(F^\times) \cong \mathbb{Z}$. In this case we normalize v by replacing it with an equivalent valuation such that $v(F^\times) = \mathbb{Z}$. Each element $\pi \in F$ with $v(\pi) = 1$ is a **prime element** of O_v.

Prime elements of a unique factorization domain R produce discrete valuations of $F = \mathrm{Quot}(R)$. If p is a prime element of R, then every element x of $F^\times$ has a unique representation as $x = up^m$, where u is relatively prime to p and $m \in \mathbb{Z}$. Define $v_p(x)$ to be m. Then v_p is a discrete valuation of F. Suppose p' is another prime element of R. Then $v_{p'}$ is equivalent to v_p if and only if $p'R = pR$, that is if $p' = up$ with $u \in R^\times$.

Example 2.2.1: Basic examples of discrete valuations.

(a) The ring of integers $\mathbb{Z}$ is a unique factorization domain. For each prime number p the residue field of $\mathbb{Q}$ at v_p is $\mathbb{F}_p$. When p ranges over all prime numbers, v_p ranges over all valuations of $\mathbb{Q}$ (Exercise 3).

(b) Let $R = K[t]$ be the ring of polynomials in an indeterminate t over a field K. Then R is a unique factorization domain. Then prime elements of R are the irreducible polynomials p over K. Units of R are the elements u of $K^\times$, so $v_p(u) = 0$ and we say v_p is **trivial** on K. The residue field of $K(t)$ at v_p is isomorphic to the field $K(a)$, where a is a root of p.

There is one additional valuation, v_∞, of $K(t)$ which is trivial on K. It is defined for a quotient $\frac{f}{g}$ of elements of $K[t]$ by the formula $v_\infty(\frac{f}{g}) = \deg(g) - \deg(f)$. The set of v_p's and v_∞ give all valuation of $K(t)$ trivial on K. Thus, all valuations of $K(t)$ which are trivial on K are discrete (Exercise 4).

An arbitrary irreducible polynomial p may have several roots $a \in \tilde{K}$. Each of them defines a place $\varphi_a\colon K(t) \to \tilde{K} \cup \{\infty\}$ by $\varphi_a(t) = a$ and $\varphi_a(c) = c$ for each $c \in K$. These places are equivalent. If $p(t) = t - a$, then φ_a is the unique place of $K(t)$ corresponding to v_p. Similarly, there is a unique place φ_∞ corresponding to v_∞. It is defined by $\varphi_\infty(t) = \infty$.

We may view each $f(t) \in K(t)$ as a function from $K \cup \{\infty\}$ into itself: $f(a) = \varphi_a(f(t))$. Explicitly, write $f(t) = \frac{g(t)}{h(t)}$ with $g, h \in K[X]$ and $\gcd(g, h) = 1$. Let $a \in K$. Then $f(a) = \frac{g(a)}{h(a)}$ if $h(a) \neq 0$ and $f(a) = \infty$

if $h(a) = 0$. To compute $f(\infty)$ let $u = t^{-1}$ and write $f(t) = \frac{g_1(u)}{h_1(u)}$ with $g_1, h_1 \in K[X]$ and $\gcd(g_1, h_1) = 1$. Then $f(\infty) = \frac{g_1(0)}{h_1(0)}$ if $h_1(0) \neq 0$ and $f(\infty) = \infty$ if $h_1(0) = 0$.

Suppose for example $f(t) \in K[t]$ and $f \neq 0$. Then f maps K into itself and $f(\infty) = \infty$. Now suppose $f(t) = \frac{at+b}{ct+d}$ with $ad - bc \neq 0$ and $c \neq 0$, then $f(\infty) = \frac{a}{c}$.

When K is algebraically closed, each irreducible polynomial is linear. Hence, each valuation of $K(t)$ which is trivial over K is either v_{t-a} for some $a \in K$ or v_∞. □

More examples of discrete valuations arise through extensions of the basic examples (Section 2.3).

LEMMA 2.2.2: *Every discrete valuation ring R is a principal ideal domain.*

Proof: Let v be the valuation of $K = \mathrm{Quot}(R)$ with $O_v = R$ and $v(K^\times) = \mathbb{Z}$. Choose a prime element π of R. Now consider a nonzero ideal $\mathfrak{a}$ of R. Then the minimal integer m with $\pi^m \in \mathfrak{a}$ is positive. It satisfies, $\mathfrak{a} = \pi^m R$. □

As a consequence of Lemma 2.2.2, finitely generated modules over R have a simple structure.

PROPOSITION 2.2.3: *Let R be a discrete valuation ring, p a prime element of R, $K = \mathrm{Quot}(R)$, and M a finitely generated R-module. Put $\bar{K} = R/pR$. Let $r = \dim_K M \otimes_R K$, $n = \dim_{\bar{K}} M/pM$, and $m = n - r$. Then there is a unique m-tuple of positive integers $(k_1, k_2, \ldots, k_m)$ with $k_1 \leq k_2 \leq \cdots \leq k_m$ and $M \cong R/p^{k_m}R \oplus \cdots \oplus R/p^{k_1}R \oplus R^r$. Moreover, r is the maximal number of elements of M which are linearly independent over R and n is the minimal number of generators of M.*

Proof: By Lemma 2.2.2, R is a principal ideal domain, so $M = M_{\mathrm{tor}} \oplus N$, where $M_{\mathrm{tor}} = \{m \in M \mid rm = 0 \text{ for some } r \in R,\ r \neq 0\}$ and N is a free R-module [Lang7, p. 147, Thm. 7.3]. Both M_{tor} and N are finitely generated [Lang7, p. 147, Cor. 7.2]. In particular, $N \cong R^s$ for some integer $s \geq 0$. Suppose $m \in M_{\mathrm{tor}}$ and $am = 0$ with $a \in R$, $a \neq 0$. Then, $m \otimes 1 = am \otimes \frac{1}{a} = 0$. Hence, $M_{\mathrm{tor}} \otimes_R K = 0$ and $M \otimes_R K \cong K^s$. Therefore, $s = r$.

By [Lang7, p. 151, Thm. 7.7], $M_{\mathrm{tor}} \cong R/q_{m'}R \oplus \cdots \oplus R/q_1 R$ where $q_1, \ldots, q_{m'}$ are elements of R which are neither zero nor units and $q_i | q_{i+1}$, $i = 1, \ldots, m' - 1$. Multiplying each q_i by a unit, we may assume $q_i = p^{k_i}$ with k_i an integer and $1 \leq k_1 \leq k_2 \leq \cdots \leq k_{m'}$. Moreover, the above cited theorem assures $Rq_1, \ldots, Rq_{m'}$ are uniquely determined by the above conditions. Hence, $k_1, \ldots, k_{m'}$ are also uniquely determined.

Combining the first two paragraphs gives:

$$M \cong R/p^{k_{m'}}R \oplus \cdots \oplus R/p^{k_1}R \oplus R^r.$$

Hence, $M/pM = (R/pR)^{m'+r} \cong \bar{K}^{m'+r}$, so $n = m' + r$ and $m' = m$.

Now recall that elements $v_1, \dots, v_s$ of M are **linearly independent** over R if $\sum_{i=1}^{s} a_i v_i = 0$ with $a_1, \dots, a_s \in R$ implies $a_1 = \cdots = a_s = 0$. Alternatively, $v_1 \otimes 1, \dots, v_s \otimes 1$ are linearly independent over K. Thus, r is the maximal number of R-linearly independent elements of M.

Finally, by Nakayama's lemma [Lang7, p. 425, Lemma 4.3], n is the minimal number of generators of M. □

Definition 2.2.4: Let R be an integral domain with quotient field F. An **overring** of R is a ring $R \subseteq R' \subset F$. It is said to be **proper** if $R \neq R'$. □

LEMMA 2.2.5: *A discrete valuation ring O has no proper overrings.*

Proof: Let R be an overring of O. Assume there exists $x \in R \setminus O$. Then x^{-1} is a nonunit of O. Choose a prime element π for O. Then $x = u\pi^{-m}$ for some $u \in O^\times$ and a positive integer m. Hence, $\pi^{-1} = u^{-1}\pi^{m-1}x \in R$. Therefore, $u'\pi^k \in R$ for all $u' \in O^\times$ and $k \in \mathbb{Z}$. We conclude that $R = \mathrm{Quot}(O)$. □

Composita of places attached to discrete valuations of rational function fields of one variable give rise to useful places of rational function fields of several variables.

Construction 2.2.6: Composition of places. Suppose ψ is a place of a field K with residue field L and φ is a place of L with residue field M. Then $\psi^{-1}(O_\varphi)$ is a valuation ring of K with maximal ideal $\psi^{-1}(\mathfrak{m}_\varphi)$ and residue field $\psi^{-1}(O_\varphi)/\psi^{-1}(\mathfrak{m}_\varphi) \cong O_\varphi/\mathfrak{m}_\varphi \cong M$. Define a map $\varphi \circ \psi\colon K \to M \cup \{\infty\}$ as follows: $\varphi \circ \psi(x) = \varphi(\psi(x))$ if $\psi(x) \neq \infty$ and $\varphi \circ \psi(x) = \infty$ if $\psi(x) = \infty$. Then $\varphi \circ \psi$ is a homomorphism on $\psi^{-1}(O_\varphi)$ and $\{x \in K \mid \varphi \circ \psi(x) = \infty\} = K \setminus \psi^{-1}(O_\varphi)$. Therefore, $\varphi \circ \psi$ is a place of K, called the **compositum** of ψ and φ, $O_{\varphi\circ\psi} = \psi^{-1}(O_\varphi)$, and $\mathfrak{m}_{\varphi\circ\psi} = \psi^{-1}(\mathfrak{m}_\varphi)$.

$$
\begin{array}{ccccc}
K & \xrightarrow{\psi} & L \cup \{\infty\} & \xrightarrow{\varphi} & M \cup \{\infty\} \\
| & & | & & | \\
O_\psi & \xrightarrow{\psi} & L & \xrightarrow{\varphi} & M \cup \{\infty\} \\
| & & | & & | \\
O_{\varphi\circ\psi} & \xrightarrow{\psi} & O_\varphi & \xrightarrow{\varphi} & M \\
| & & | & & | \\
\mathfrak{m}_{\varphi\circ\psi} & \xrightarrow{\psi} & \mathfrak{m}_\varphi & \xrightarrow{\varphi} & 0 \\
| & & | & & | \\
\mathfrak{m}_\psi & \xrightarrow{\psi} & 0 & \xrightarrow{\varphi} & 0
\end{array}
$$

In addition, $L = \bar{K}_\psi$ and $M = \bar{L}_\varphi = \bar{K}_{\varphi\circ\psi}$. □

LEMMA 2.2.7: *Let K be a field, $a_1, \dots, a_r$ elements of $\tilde{K}$, $t_1, \dots, t_r$ indeterminates, and L a finite extension of K. Then there exists a K-place $\varphi\colon K(\mathbf{t}) \to K(\mathbf{a}) \cup \{\infty\}$ such that $\varphi(t_i) = a_i$, $i = 1, \dots, r$. Moreover, every extension of φ to an L-place of $L(\mathbf{t})$ maps $L(\mathbf{t})$ onto $L(\mathbf{a}) \cup \{\infty\}$.*

Proof: For each i there is a $K(a_1, \dots, a_{i-1}, t_{i+1}, \dots, t_r)$-place

$$\varphi_i\colon K(a_1, \dots, a_{i-1}, t_i, t_{i+1} \dots, t_r) \to K(a_1, \dots, a_{i-1}, a_i, t_{i+1}, \dots, t_r)$$

with $\varphi_i(t_i) = a_i$ (Example 2.2.1). The compositum $\varphi = \varphi_r \circ \cdots \circ \varphi_1$ is a K-place of $K(t_1, \ldots, t_r)$ with residue field $K(a_1, \ldots, a_r)$ and $\varphi(t_i) = a_i$, $i = 1, \ldots, r$.

Let now φ be an extension of φ to an L-place of $L(\mathbf{t})$. Choose a basis $b_1, \ldots, b_n$ for L/K. Then $b_1, \ldots, b_n$ is also a basis for $L(\mathbf{t})/K(\mathbf{t})$. Hence, each $f \in L(\mathbf{t})$ has a presentation $f = \sum_{i=1}^{n} b_i f_i$ with $f_i \in K(\mathbf{t})$. Assume without loss that $\frac{f_i}{f_1}$ is finite under φ for $i = 1, \ldots, n$. Then $f = f_1 \sum_{i=1}^{n} \frac{f_i}{f_1} b_i$ and $\varphi(f) \in L(a_1, \ldots, a_r) \cup \{\infty\}$. Thus, $\varphi(L(\mathbf{t})) = L(\mathbf{a}) \cup \{\infty\}$. □

2.3 Extensions of Valuations and Places

The examples of Section 2.2 and the following extension results give a handle on describing valuations of function fields in one variable.

PROPOSITION 2.3.1 (Chevalley [Lang4, p. 8, Thm. 1]): *Let φ_0 be a homomorphism of an integral domain R into an algebraically closed field M and let F be a field containing R. Then φ_0 extends either to an embedding φ of F into M or to a place φ of F into $M \cup \{\infty\}$.*

When F is algebraic over R, the proposition has a more precise form:

Let $f \in R[X]$ be an irreducible polynomial over $E = \mathrm{Quot}(R)$ and $\bar{f} \in M[X]$ the result of applying φ_0 to the coefficients of f. Suppose $\bar{f}$ is not identically zero. Assume x and $\bar{x}$ are roots of f and $\bar{f}$ in $\tilde{E}$ and M, respectively. Then φ_0 extends to a place φ of $E(x)$ into $M \cup \{\infty\}$ with $\varphi(x) = \bar{x}$ [Lang4, p. 10, Thm. 2]. *Moreover, if φ_0 is injective, so is φ* [Lang4, p. 8, Prop. 2].

In particular, suppose v is a valuation of a field E and F is an extension of E. Then v extends to a valuation w_0 of F. Each valuation w of F which is equivalent to w_0 **lies over** v. Thus, w lies over v if and only if $O_v \subseteq O_w$ and $\mathfrak{m}_v = \mathfrak{m}_w \cap O_v$. The number $e_{w/v} = (w(F^\times) : w(E^\times))$ is the **ramification index** of w **over** v (and also over E). The field degree $[F : E]$ bounds $e_{w/v}$ (Exercise 5). Similarly, $\bar{E}_v$ embeds in $\bar{F}_w$ to give the inequality $f_{w/v} = [\bar{F}_w : \bar{E}_v] \leq [F : E]$ (Exercise 7). Both the ramification index and the residue field degree are multiplicative. Thus, if (F', w') is an extension of (F, w), then $e_{w'/v} = e_{w'/w} e_{w/v}$ and $f_{w'/v} = f_{w'/w} f_{w/v}$. If $[F : E] < \infty$, then the number of valuations of F that lie over v is finite (a consequence of Proposition 2.3.2).

PROPOSITION 2.3.2: *Let F/E be a finite extension of fields and v a valuation of E. Let $w_1, \ldots, w_g$ be all inequivalent extensions of v to F. Then*

$$\sum_{i=1}^{g} e_{w_i/v} f_{w_i/v} \leq [F : E] \tag{1}$$

[Bourbaki2, p. 420, Thm. 1]. If, in addition, v is discrete and F/E is separa-

ble, then each w_i is discrete and (see [Bourbaki2, p. 425, Cor. 1])

$$\sum_{i=1}^{g} e_{w_i/v} f_{w_i/v} = [F : E]. \tag{2}$$

Suppose $(F, w)/(E, v)$ is an extension of discrete valued fields. In particular, $w(a) = v(a)$ for each $a \in E$. By definition, $e_{w/v} = (w(F^\times) : v(E^\times))$. However, as in Section 2.2, it is customary to replace v and w by equivalent valuations with $v(E^\times) = w(F^\times) = \mathbb{Z}$. The new valuations satisfy

$$w(a) = e_{w/v} v(a) \quad \text{for each} \quad a \in E.$$

Whenever we speak about an extension of discrete valuations, we mean they are normalized and satisfy the latter relation.

Suppose F is a finite Galois extension of E with a Galois group G. Let w be a discrete valuation of F and let $\sigma \in G$. Then, $\sigma(w)$ is a valuation of F (Section 2.1), both w and $\sigma(w)$ lie over the same valuation v of E, and

$$e_{w/v} = e_{\sigma(w)/v} \quad \text{and} \quad f_{w/v} = f_{\sigma(w)/v}.$$

Conversely, suppose w and w' are two discrete valuations of F over the same valuation v of E. Then there exists $\sigma \in G$ such that $\sigma(w) = w'$ (Exercise 9). Thus, if $w_1, \ldots, w_g$ are all distinct valuations of F that lie over v, then they all have the same residue degree f and ramification index e over v. In this case formula (2) simplifies to

$$efg = [F : E]. \tag{3}$$

The subgroups

$$D_w = D_{w/v} = \{\sigma \in G \mid \ \sigma O_w = O_w\}$$
$$I_w = I_{w/v} = \{\sigma \in G \mid \ w(x - \sigma x) > 0 \text{ for all } x \in O_w\}$$

are the **decomposition group** and the **inertia group**, respectively, of w over E. Obviously $I_w \lhd D_w$. If $\bar{F}_w/\bar{E}_v$ is separable, then [Serre3, p. 33]

$$|I_w| = e_{w/v} \quad \text{and} \quad |D_w| = e_{w/v} f_{w/v}. \tag{4}$$

Section 2.6 generalizes the notion of separable algebraic extension of fields to arbitrary extensions of fields. In particular, purely transcendental extensions of fields are separable. We use this notion in the following definition. Suppose $(F, w)/(E, v)$ is an arbitrary extension of valued fields. We say w is **unramified** (resp. **tamely ramified**) over v (or also over E) if $\bar{F}_w/\bar{E}_v$ is a separable extension and $e_{w/v} = 1$ (resp. $\mathrm{char}(\bar{E}_v) \nmid e_{w/v}$). We say v is **unramified** (resp. **tamely ramified**) in F if each extension of v to F is unramified (resp. tamely ramified) over v.

Example 2.3.3: Purely transcendental extensions. Let (E, v) be a valued field. Consider a transcendental element t over E. Extend v to a valuation v' of $E(t)$ as follows.

First define v' on $E[t]$ by the following rule:

$$v'\big(\sum_{i=0}^{m} a_i t^i\big) = \min\big(v(a_0), \dots, v(a_m)\big) \tag{5}$$

for $a_0, \dots, a_m \in E$. The same argument used to prove Gauss' Lemma proves that $v'(fg) = v'(f) + v'(g)$ for all $f, g \in E[t]$.

Indeed, let $f(t) = \sum_{i=0}^{m} a_i t^i$ and $g(t) = \sum_{j=0}^{n} b_j t^j$. Let r be the minimal integer with $v(a_r) = \min\big(v(a_0), \dots, v(a_m)\big)$ and let s be the minimal integer with $v(b_s) = \min\big(v(b_0), \dots, v(b_n)\big)$. If $i + j = r + s$ and $(i, j) \neq (r, s)$, then either $i < r$ or $j < s$. In both cases $v(a_r) + v(b_s) < v(a_i) + v(b_j)$. Hence

$$\begin{aligned} v'\big(\sum_{i=0}^{m} a_i t^i\big) + v'\big(\sum_{j=0}^{n} b_j t^j\big) &= v(a_r) + v(b_s) \\ &= \min\big(\sum_{i+j=k} v(a_i b_j) \mid k = 0, \dots, m+n\big) \\ &= v'\big(\sum_{i=0}^{m} a_i t^i \cdot \sum_{j=0}^{n} b_j t^j\big), \end{aligned}$$

as claimed.

We extend v' to $E(t)$ by the rule $v'(\frac{f}{g}) = v'(f) - v'(g)$. Then we prove $v'(u_1 + u_2) \geq \min\big(v'(u_1), v'(u_2)\big)$ first for $u_1, u_2 \in E[t]$ and then for $u_1, u_2 \in E(t)$. Thus, v' is a valuation of $E(t)$. Note that the residue of t at v' is transcendental over $\bar{E}_v$. Indeed, suppose $\sum_{i=0}^{n} \bar{a}_i \bar{t}^i = 0$ for some $a_0, \dots, a_n \in O_v$. Then $\min\big(v(a_0), \dots, v(a_n)\big) = v'\big(\sum_{i=0}^{n} a_i t^i\big) > 0$. Hence, $\bar{a}_i = 0$, $i = 0, \dots, n$.

It follows that, $\overline{E(t)}_{v'} = \bar{E}_v(\bar{t})$ is a rational function field over $\bar{E}_v$. By definition, $\Gamma_{v'} = \Gamma_v$. In particular, if v is discrete, then so is v' and $e_{v'/v} = 1$.

Suppose v'' is another extension of v to $E(t)$ with the residue of t at v'' transcendental over $\bar{E}_v$. We show that $v'' = v'$. Indeed, for $a_0, \dots, a_n \in E$, not all zero, choose j between 0 and n with $v(a_j) = \min\big(v(a_0), \dots, v(a_n)\big)$. Then $\sum_{i=0}^{n} \overline{a_i/a_j} \bar{t}^i \neq 0$. Therefore,

$$\begin{aligned} v''\big(\sum_{i=0}^{n} a_i t^i\big) &= v(a_j) + v''\big(\sum_{i=0}^{n} (a_i/a_j) t^i\big) \\ &= \min\big(v(a_0), \dots, v(a_n)\big) = v'\big(\sum_{i=0}^{n} a_i t^i\big), \end{aligned}$$

as claimed. □

LEMMA 2.3.4: *Let v be a discrete valuation of a field E, $h \in O_v[X]$ a monic irreducible polynomial of degree n, x a root of $h(X)$ in $\tilde{E}$, and $F = E(x)$. Suppose the residue polynomial $\bar{h}(X)$ is separable. Then v is unramified in F.*

Proof: By assumption, $\bar{h}(X) = \prod_{i=1}^{r} h_i(X)$, where $h_i \in \bar{E}_v[X]$ are distinct monic irreducible polynomials. For each i between 1 and r choose a root a_i of $h_i(X)$ in $(\bar{E}_v)_s$. Use Proposition 2.3.1 to extend the residue map $O_v \to \bar{E}_v$ to a place φ_i of F with $\varphi_i(x) = a_i$. Denote the corresponding valuation by w_i. Then $\bar{E}_v(a_i) \subseteq \bar{F}_{w_i}$. Since $h_i(X)$ and $h_j(X)$ have no common root for $i \neq j$, the valuations $w_1, \ldots, w_r$ are mutually inequivalent extensions of v. Label any further extensions of v to valuations of F as $w_{r+1}, \ldots, w_g$. By (1)

$$n = \sum_{i=1}^{r} \deg(h_i) = \sum_{i=1}^{r} [\bar{E}_v(a_i) : \bar{E}_v] \leq \sum_{i=1}^{g} e_{w_i/v} f_{w_i/v} \leq n.$$

Hence, $e_{w_i/v} = 1$ and $\bar{E}_v(a_i) = \bar{F}_{w_i}$ for $i = 1, \ldots, r$. Moreover, $w_1, \ldots, w_r$ are all extensions of v to F and each of them is unramified over E. Therefore, v is unramified in F. □

The converse of Lemma 2.3.4 requires $\bar{E}_v$ to be infinite.

LEMMA 2.3.5: *Let v be a discrete valuation of a field E. Let F be a separable extension of E of degree n. Suppose v is unramified in F and $\bar{E}_v$ is an infinite field. Then F/E has a primitive element x with* $\operatorname{irr}(x, E) \in O_v[X]$ *and the residue of* $\operatorname{irr}(x, E)$ *at v is a separable polynomial.*

Proof: Let $w_1, \ldots, w_g$ be all extensions of v to F. By (2), $[F : E] = \sum_{i=1}^{g} [\bar{F}_{w_i} : \bar{E}_v]$. Moreover, for each i the extension $\bar{F}_{w_i}/\bar{E}_v$ is finite and separable. Hence, we may choose c_i in F with $w_i(c_i) = 0$ and the residue $\bar{c}_i$ of c_i at w_i is a primitive element of $\bar{F}_{w_i}/\bar{E}_v$. Let $h_i = \operatorname{irr}(\bar{c}_i, \bar{E}_v)$. Since $\bar{E}_v$ is infinite, we may choose $c_1, \ldots, c_g$ such that $\bar{c}_1, \ldots, \bar{c}_g$ are mutually nonconjugate over $\bar{E}_v$. Thus, $h_1, \ldots, h_g$ are relatively prime.

Use Proposition 2.1.1 to find $x \in F$ with $w_i(x - c_i) > 0$, $i = 1, \ldots, g$. Then, $w_i(x) = 0$, $i = 1, \ldots, g$. Extend each w_i to the Galois closure of F/E. Then all E-conjugates of x have nonnegative values under each extended valuation. Hence, the elementary symmetric polynomials in the E-conjugates of x belong to O_v. Therefore, $f(X) = \operatorname{irr}(x, E) \in O_v[X]$.

Let $\bar{f}$ be the residue of f at v. By construction, $\bar{f}(\bar{c}_i) = 0$, therefore $h_i | \bar{f}$, $i = 1, \ldots, g$. Since $h_1, \ldots, h_g$ are relatively prime, $\prod_{i=1}^{g} h_i | \bar{f}$. Hence,

$$\begin{aligned}[F : E] = \sum_{i=1}^{g} [\bar{F}_{w_i} : \bar{E}_v] &= \sum_{i=1}^{g} \deg(h_i) \\ &\leq \deg(\bar{f}) = \deg(f) = [E(x) : E] \leq [F : E].\end{aligned}$$

Consequently, $E(x) = F$, as desired. □

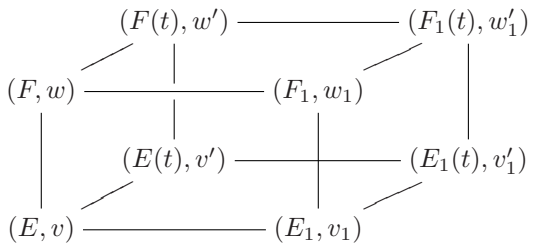
Example 3.5.4 shows the assumption on $\bar{E}_v$ to be infinite is necessary for Lemma 2.3.5 to hold.

The next lemma says that arbitrary change of the base field preserves unramified discrete valuations.

LEMMA 2.3.6: *Let (E, v) be a discrete valued field. Consider a separable algebraic extension F of E and a discrete valued field (E_1, v_1) which extends (E, v). Suppose v is unramified in F. Then v_1 is unramified in FE_1.*

Proof: Suppose without loss that $[F : E] < \infty$. Let $F_1 = FE_1$. Suppose first that $\bar{E}_v$ is infinite. Choose x as in Lemma 2.3.5 and let $f(X) = \mathrm{irr}(x, E)$. Then $F = E(x)$ and $\bar{f}(X)$ is separable. Hence, $F_1 = E_1(x)$ and $\bar{f}(X)$ is still separable. By Lemma 2.3.4, v_1 is unramified in F_1.

In the general case we consider an extension w_1 of v_1 to a valuation of F_1. Denote the restriction of w_1 to F by w. Let t be transcendental over F_1. Example 2.3.3 extends v (resp. w, v_1, w_1) in a canonical way to a discrete valuation v' (resp. w', v_1', w_1') of $E(t)$ (resp. $F(t)$, $E_1(t)$, $F_1(t)$). Further, $e_{v'/v} = 1$ (resp. $e_{w'/w} = 1$, $e_{v_1'/v_1} = 1$, $e_{w_1'/w_1} = 1$) and $\overline{E(t)}_{v'} = \bar{E}_v(\bar{t})$ (resp. $\overline{F(t)}_{w'} = \bar{F}_w(\bar{t})$, $\overline{E_1(t)}_{v_1'} = \bar{E}_{1,v_1}(\bar{t})$, $\overline{F_1(t)}_{w_1'} = \bar{F}_{1,w_1}(\bar{t})$), where $\bar{t}$ is transcendental over $\bar{F}_{1,w_1}$. Moreover, w_1' extends w' and v_1' extends v' giving this diagram:



We claim v' is unramified in $F(t)$. Indeed, $\overline{F(t)}_{w'} = \bar{F}_w \cdot \bar{E}_v(\bar{t})$ is a separable extension of $\overline{E(t)}_{v'}$. Also, $e_{w'/v'} = e_{w'/v'}e_{v'/v} = e_{w'/v} = e_{w'/w}e_{w/v} = 1$. Hence, w' is unramified over v'. If u^* is an arbitrary extension of v' to $F(t)$ and u is its restriction to F, then the residue of t at u^* is $\bar{t}$, which is transcendental over $\bar{F}_u$. Thus, by uniqueness of the construction in Example 2.3.3, $u^* = u'$, where u' is the canonical extension of u to $F(t)$. By the above, u^* is unramified over v'.

Since $\overline{E(t)}_{v'}$ is infinite, the first paragraph of the proof implies v_1' is unramified in $F_1(t)$. Thus, $\bar{F}_{1,w_1}(\bar{t})/\bar{E}_{1,v_1}(\bar{t})$ is a separable extension and $e_{w_1'/v_1'} = 1$. Therefore, $\bar{F}_{1,w_1}/\bar{E}_{1,v_1}$ is a separable extension and

$$e_{w_1/v_1} = e_{w_1/v_1}e_{w_1'/w_1} = e_{w_1'/v_1} = e_{w_1'/v_1'}e_{v_1'/v_1} = 1.$$

Consequently, v_1 is unramified in F_1. □

Combine the multiplicativity of the ramification index and the residue field degree with Lemma 2.3.6 to prove:

COROLLARY 2.3.7: *Let $(E,v) \subseteq (E',v') \subseteq (E'',v'')$ be a tower of discrete valued fields. The following hold:*
(a) *v''/v is unramified if and only if v''/v' and v'/v are unramified.*
(b) *v is unramified in E'' if and only if v is unramified in E' and each extension of v to E' is unramified in E''.*
(c) *Let F_1 and F_2 be field extensions of E which are contained in a common field. Suppose F_1/E is separable algebraic and v is unramified in F_1 and in F_2. Then v is unramified in F_1F_2.*

Example 2.3.8: Radical extensions. Let (E,v) be a discrete valued field and n a positive integer with $\mathrm{char}(\bar{E}_v) \nmid n$. Consider an extension $F = E(x)$ of degree n of E where $x^n = a$ is in E. Let w be an extension of v to a valuation of F and let $e = e_{w/v}$. Assume both v and w are normalized. Then

$$nw(x) = ev(a) \quad \text{and} \quad e \leq n. \tag{6}$$

There are three cases to consider:

CASE A: $\gcd\big(n, v(a)\big) = 1$. By (6), $n|e$, so $n = e$. By (2), w is the unique extension of v to F. Therefore, v **totally ramifies** in F.

CASE B: $n \nmid v(a)$. By (6), $e \neq 1$. Hence, w ramifies over E.

CASE C: $n|v(a)$. Choose $\pi \in E$ with $v(\pi) = 1$. Write $a = b\pi^{kn}$ with $k \in \mathbb{Z}$ and $b \in E$ such that $v(b) = 0$. Then $y = x\pi^{-k}$ satisfies $y^n = b$ and $F = E(y)$. Moreover, $Y^n - \bar{b}$ decomposes over $(\bar{E}_v)_s$ into distinct linear factors. Therefore, by Lemma 2.3.4, v is unramified in F. □

Example 2.3.9: Artin-Schreier Extensions. Let (E,v) be a discrete valued field of positive characteristic p. An **Artin-Schreier extension** F of degree p has the form $E(x)$ where $x^p - x = a$ with $a \in E$. We consider two cases:

CASE A: *$v(a) < 0$ and $p \nmid v(a)$.* Let w be an extension of v to F. Then $w(x)$ must be negative and $w(x^p) < w(x)$. Hence, $pw(x) = ev(a)$, where $e = e_{w/v}$. Hence, $p = e$ and $w(x) = v(a)$. Thus, v totally ramifies in F.

CASE B: $v(a) \geq 0$. Then $X^p - X - \bar{a}$ is a separable polynomial. By Lemma 2.3.4, v is unramified in F.

In particular, if $v(a) > 0$, then $X^p - X = \prod_{i=0}^{p-1}(X-i)$ in $\bar{E}_v$. Hence, by Proposition 2.3.2, v has exactly p extensions to F. Label them $v_0, \ldots, v_{p-1}$ with $v_i(x-i) > 0$, $i = 0, \ldots, p-1$. Since $v_i(x-i) < v_i\big((x-i)^p\big)$, we conclude from $(x-i)^p - (x-i) = a$ that $v_i(x-i) = v(a)$. □

LEMMA 2.3.10 (Eisenstein's Criterion): *Let R be a unique factorization domain, p a prime element of R, and $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ a polynomial with coefficients $a_i \in R$. Then each of the following conditions suffices for f to be irreducible over* $\mathrm{Quot}(R)$*:*
(a) *$p \nmid a_n$, p divides $a_0, \ldots, a_{n-1}$, and $p^2 \nmid a_0$.*

(b) *$p \nmid a_0$, p divides $a_1, \dots, a_n$, and $p^2 \nmid a_n$.*

Proof of (a): See [Lang7, p. 183].

Proof of (b): By (a), the polynomial $X^n f(X^{-1}) = a_n + a_{n-1}X + \cdots + a_0 X^n$ is irreducible over K. Therefore, $f(X)$ is irreducible. □

Example 2.3.11: Ramification at infinity. Let K be a field, t an indeterminate, and $f(X) = a_n X^n + \cdots + a_0 \in K[X]$ with $a_n \neq 0$. By Eisenstein criterion, $f(X) - t$ is irreducible over $\tilde{K}(t)$. Choose a root x of $f(X) = t$ in $\widetilde{K(t)}$. Let $v = v_\infty$ be the valuation of $K(t)$ with $v(t) = -1$ which is trivial on K and let w be a valuation of $K(x)$ lying over v. The relation $a_n x^n + \cdots + a_0 = t$ implies $w(x) < 0$. Hence, $-e_{w/v} = w(t) = w(f(x)) = nw(x)$. Since $e_{w/v} \leq [K(x) : K(t)] \leq n$, this implies $e_{w/v} = [K(x) : K(t)] = n$ and $w(x) = -1$. Hence, v is totally ramified in $K(x)$. In particular, w is the unique valuation of $K(x)$ lying over $K(t)$. □

2.4 Integral Extensions and Dedekind Domains

Integral extensions of $\mathbb{Z}$ in number fields are Dedekind domains. Although they are in general not unique factorization domain, their ideals uniquely factor as products of prime ideals. In this section we survey the concepts of integral extensions of rings and of Dedekind domains and prove that every overring of a Dedekind domain is again a Dedekind domain.

Let F be a field containing an integral domain R. An element $x \in F$ is **integral over** R if it satisfies an equation of the form $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ with $a_1, \dots, a_n \in R$. The set of all elements of F which are integral over R form a ring (e.g. by Proposition 2.4.1 below), the **integral closure** of R in F. Call R **integrally closed** if R coincides with its integral closure in $\mathrm{Quot}(R)$. For example, every valuation ring O of F is integrally closed. Indeed, assume $x \in F \setminus O$ and x is integral over O. Then $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ for some $a_0, \dots, a_{n-1} \in O$. Then x^{-1} is in the maximal ideal $\mathfrak{m}$ of O and $1 + a_{n-1}x^{-1} + \cdots + a_0 x^{-n} = 0$. Thus, $1 \in \mathfrak{m}$, a contradiction.

Proposition 2.4.1 ([Lang4, p. 12]): *An element x of F is integral over R if and only if every place of F finite on R is finite at x. Thus, the integral closure of R in F is the intersection of all valuation rings of F which contain R. In particular, every valuation ring of F is integrally closed.*

Suppose φ is a place of a field F and K is a subfield of F. We say that φ is **trivial** on K, or also that φ is a place of F/K, if $\varphi(x) \neq \infty$ for all $x \in K$. Then $\varphi(y) \neq 0$ for all $y \in K^\times$. Thus, φ maps K isomorphically onto $\varphi(K)$.

Lemma 2.4.2: *Let $K \subseteq L \subseteq F$ be a tower of fields and φ a place of F. Suppose φ is trivial on K and L is algebraic over K. Then φ is trivial on L.*

Proof: Each $x \in L$ is integral over K, so by Proposition 2.4.1, $\varphi(x) \neq \infty$. Thus, φ is also trivial on L. □

Let S be a subring of F containing R. Call S **integral over** R if every element of S is integral over R. If $S = R[x_1, \ldots, x_m]$ and S is integral over R, then S is a finitely generated R-module. Indeed, every element of S is a linear combination with coefficients in R of the set of monomials $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m}$, where $0 \le \alpha_i < \deg\big(\mathrm{irr}(x_i, \mathrm{Quot}(R))\big)$. Propositions 2.3.1 and 2.4.1 give the following:

PROPOSITION 2.4.3: *Let $R \subseteq S$ be integral domains with S finitely generated as an R-algebra. Suppose S is integral over R. Then the following hold:*
(a) *S is finitely generated as an R-module.*
(b) *Let $\varphi\colon R \to M$ be a homomorphism into an algebraically closed field M. Then the set of all homomorphisms $\psi\colon S \to M$ that extend φ is finite and nonempty.*

Suppose $R_1 \subseteq R_2 \subseteq R_3$ are integral domains. Proposition 2.4.1 implies that R_3 is integral over R_1 if and only if R_2 is integral over R_1 and R_3 is integral over R_2.

Call an integral domain R **Noetherian** if every ideal of R is finitely generated. For example, since a discrete valuation ring O is a principal ideal domain, it is integrally closed and Noetherian.

If R is an integral domain and $\mathfrak{p}$ is a prime ideal of R, then

$$R_{\mathfrak{p}} = \Big\{ \frac{a}{b} \mid a \in R \quad \text{and} \quad b \in R \smallsetminus \mathfrak{p} \Big\}$$

is the **local ring** of R at $\mathfrak{p}$. It has a unique maximal ideal, $\mathfrak{p}R_{\mathfrak{p}}$. If R is a Noetherian domain, then $R_{\mathfrak{p}}$ is also Noetherian. If R is integrally closed, then so is $R_{\mathfrak{p}}$.

LEMMA 2.4.4: *Suppose R is an integral domain. Then $R = \bigcap R_{\mathfrak{m}}$, where $\mathfrak{m}$ ranges over all maximal ideals of R. More generally, $\mathfrak{a} = \bigcap \mathfrak{a}R_{\mathfrak{m}}$ for each ideal $\mathfrak{a}$ of R.*

Proof: Suppose x belongs to each $\mathfrak{a}R_{\mathfrak{m}}$. For each $\mathfrak{m}$, $x = a_{\mathfrak{m}}/b_{\mathfrak{m}}$, with $a_{\mathfrak{m}} \in \mathfrak{a}$ and $b_{\mathfrak{m}} \in R \smallsetminus \mathfrak{m}$. Denote the ideal generated by all the $b_{\mathfrak{m}}$'s by $\mathfrak{b}$. If $\mathfrak{b} \neq R$, then $\mathfrak{b}$ is contained in a maximal ideal $\mathfrak{m}$. Hence, $b_{\mathfrak{m}} \in \mathfrak{m}$, a contradiction. Hence, $\mathfrak{b} = R$. In particular, $1 = \sum_{\mathfrak{m} \in M} b_{\mathfrak{m}} c_{\mathfrak{m}}$ where M is a finite set of maximal ideals, and $c_{\mathfrak{m}} \in R$ for each $\mathfrak{m} \in M$. Therefore $x = \sum_{\mathfrak{m} \in M} x b_{\mathfrak{m}} c_{\mathfrak{m}} = \sum_{\mathfrak{m} \in M} a_{\mathfrak{m}} c_{\mathfrak{m}} \in \mathfrak{a}$. □

Let R be an integral domain with the quotient field F. A nonzero R-submodule $\mathfrak{a}$ of F is said to be a **fractional ideal** of R if there exists a nonzero $x \in R$ with $x\mathfrak{a} \subseteq R$. In particular, every ideal of R is a fractional ideal. Define the **product**, $\mathfrak{ab}$, of two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ to be the R-submodule generated by the products ab, with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. Define the **inverse** of a fractional ideal $\mathfrak{a}$ as $\mathfrak{a}^{-1} = \{x \in F \mid x\mathfrak{a} \subseteq R\}$. If $a \in \mathfrak{a}$, then $a\mathfrak{a}^{-1} \subseteq R$. Therefore, both $\mathfrak{ab}$ and $\mathfrak{a}^{-1}$ are fractional ideals.

PROPOSITION 2.4.5 ([Cassels-Fröhlich, p. 6]): *The following conditions on an integral domain R are equivalent:*

(a) *R is Noetherian, integrally closed, and its nonzero prime ideals are maximal.*

(b) *R is Noetherian and the local ring, $R_{\mathfrak{p}}$, of every nonzero prime ideal $\mathfrak{p}$ is a discrete valuation ring.*

(c) *Every fractional ideal $\mathfrak{a}$ is* **invertible** *(i.e. $\mathfrak{a}\mathfrak{a}^{-1} = R$).*

When these conditions hold, R is called a **Dedekind domain**.

By Proposition 2.4.5, the set of all fractional ideals of a Dedekind domain R forms an Abelian group, with R being the unit. One proves that this group is free and the maximal ideals of R are free generators of this group. Thus, every ideal $\mathfrak{a}$ of R has a unique presentation $\mathfrak{a} = \mathfrak{p}_1^{m_1}\mathfrak{p}_2^{m_2}\cdots\mathfrak{p}_r^{m_r}$, as the product of powers of maximal ideals with positive exponents [Cassels-Fröhlich, p. 8].

Every principal ideal domain is a Dedekind domain. Thus, $\mathbb{Z}$ and $K[x]$, where x is a transcendental element over a field K, are Dedekind domains. By the same reason, every discrete valuation ring is a Dedekind domain.

In the notation of Proposition 2.4.5(b), $R_{\mathfrak{p}}$ is the valuation ring of a discrete valuation $v_{\mathfrak{p}}$ of $K = \mathrm{Quot}(R)$. The corresponding place $\varphi_{\mathfrak{p}}$ is finite on R. Conversely, if φ is such a place, then $\mathfrak{p} = \{x \in R \mid \varphi(x) = 0\}$ is a nonzero prime ideal of R. Since $R_{\mathfrak{p}} \subseteq O_\varphi$, Lemma 2.2.5 implies that $R_{\mathfrak{p}} = O_\varphi$. This establishes a bijection between the nonzero prime ideals of R and the equivalence classes of places of K finite on R.

PROPOSITION 2.4.6 ([Cassels-Fröhlich, p. 13]): *Let S be the integral closure of a Dedekind domain R in a finite algebraic extension of* $\mathrm{Quot}(R)$*. Then S is also a Dedekind domain.*

Let $\mathfrak{p}$ be a prime ideal of R. Then $\mathfrak{p}S = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_r^{e_r}$, where $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_r$ are the distinct prime ideals of S that lie over $\mathfrak{p}$; that is, $\mathfrak{P}_i \cap R = \mathfrak{p}$, $i = 1, \ldots, r$. For each i we have $\mathfrak{p}S_{\mathfrak{P}_i} = \mathfrak{P}_i^{e_i}S_{\mathfrak{P}_i}$. Hence, e_i is the ramification index of $v_{\mathfrak{P}_i}$ over $v_{\mathfrak{p}}$. We say $\mathfrak{P}_i$ is **unramified** over K if $v_{\mathfrak{P}_i}/v_{\mathfrak{p}}$ is unramified; that is, $e_i = 1$ and $S/\mathfrak{P}_i$ is a separable extension of $R/\mathfrak{p}$. The prime ideal $\mathfrak{p}$ is **unramified** in L if each $\mathfrak{P}_i$ is unramified over K.

By Proposition 2.4.6, the integral closure of $\mathbb{Z}$ in a finite extension L of $\mathbb{Q}$ is a Dedekind domain, O_L, called the **ring of integers** of L.

PROPOSITION 2.4.7 (Noether-Grell): *Every overring R' of a Dedekind domain R is a Dedekind domain.*

Proof: We show that R' satisfies Condition (b) of Proposition 2.4.5.

PART A: *An injective map.* If $\mathfrak{p}'$ is a nonzero prime ideal of R', then $\mathfrak{p} = R \cap \mathfrak{p}'$ is a nonzero prime ideal of R. Indeed, for $0 \neq x \in \mathfrak{p}'$, write $x = \frac{a}{b}$, where $a, b \in R$. Thus, $0 \neq a = bx \in R \cap \mathfrak{p}' = \mathfrak{p}$. Since $R_{\mathfrak{p}} \subseteq R'_{\mathfrak{p}'}$ and $R_{\mathfrak{p}}$ is a discrete valuation ring, Lemma 2.2.5 implies that $R_{\mathfrak{p}} = R'_{\mathfrak{p}'}$. Hence,

$$\mathfrak{p}R_{\mathfrak{p}} = \mathfrak{p}'R'_{\mathfrak{p}'}. \tag{1}$$

In addition, $\mathfrak{p}'R'_{\mathfrak{p}'} \cap R' = \mathfrak{p}'$. Therefore, the map $\mathfrak{p}' \mapsto R \cap \mathfrak{p}'$ from the set of nonzero prime ideals of R' into the set of nonzero prime ideals of R is injective.

PART B: *A finiteness condition.* Let x be a nonzero element of R', $\mathfrak{p}'$ a prime ideal of R' which contains x, and $\mathfrak{p} = R \cap \mathfrak{p}'$. Then $R_{\mathfrak{p}} = R'_{\mathfrak{p}'}$. Hence, $v_{\mathfrak{p}}(x) > 0$, where $v_{\mathfrak{p}}$ is the valuation of $\mathrm{Quot}(R)$ corresponding to $\mathfrak{p}$. But this relation holds only for the finitely many prime ideals of R that appear with positive exponents in the factorization of the fractional ideal xR. Hence, by Part A, x belongs to only finitely many prime ideals of R'.

PART C: *The ring R' is Noetherian.* Let $\mathfrak{a}$ be a nonzero ideal of R'. Choose a nonzero element $x \in \mathfrak{a}$ and denote the finite set of prime ideals of R' that contain x by P. For each $\mathfrak{p} \in P$ the local ring $R'_{\mathfrak{p}}$ is a discrete valuation domain. Hence, there exists $a_{\mathfrak{p}} \in \mathfrak{a}$ such that $\mathfrak{a}R'_{\mathfrak{p}} = a_{\mathfrak{p}}R'_{\mathfrak{p}}$. Denote the ideal of R' generated by x and by all $a_{\mathfrak{p}}$, for $\mathfrak{p} \in P$, by $\mathfrak{a}_0$. It is contained in $\mathfrak{a}$. To show that $\mathfrak{a}$ is finitely generated, we need only prove that $\mathfrak{a} \subseteq \mathfrak{a}_0$.

Indeed, consider a prime ideal $\mathfrak{q}$ of R' not in P. Then $x \notin \mathfrak{q}$, so $\mathfrak{a}_0 \not\subseteq \mathfrak{q}$. Hence, $\mathfrak{a}_0 R'_{\mathfrak{q}} = R'_{\mathfrak{q}}$. It follows from Lemma 2.4.4 that $\mathfrak{a}_0 = \bigcap_{\mathfrak{p}\in P} \mathfrak{a}_0 R'_{\mathfrak{p}}$. Therefore, $\mathfrak{a} \subseteq \bigcap_{\mathfrak{p}\in P} \mathfrak{a}R'_{\mathfrak{p}} = \bigcap_{\mathfrak{p}\in P} a_{\mathfrak{p}}R'_{\mathfrak{p}} \subseteq \bigcap_{\mathfrak{p}\in P} \mathfrak{a}_0 R'_{\mathfrak{p}} = \mathfrak{a}_0$, as desired. □

LEMMA 2.4.8: *Let (E, v) be a discrete valued field, F_1, F_2, F finite separable extensions of E with $F = F_1F_2$, and w an extension of v to F. Suppose v is unramified in F_1. Then the residue fields with respect to w satisfy $\bar{F} = \bar{F}_1\bar{F}_2$.*

Proof: Choose a finite Galois extension N of E which contains F and an extension w' of w to N. Denote the decomposition groups of w' over E, F_1, F_2, F by $D_E, D_{F_1}, D_{F_2}, D_F$, respectively. Let E', F'_1, F'_2, F' be the fixed fields in N of $D_E, D_{F_1}, D_{F_2}, D_F$, respectively. Let $v' = w'|_{E'}$. Since all valuations of N lying over v' are conjugate over E', the definition of E' as the fixed field of D_E implies that w' is the unique extension of v' to N. Also, $D_{F_1} = \mathrm{Gal}(N/F_1) \cap D_E$, so $F_1E' = F'_1$. By Lemma 2.3.6, v' is unramified in F'_1. Finally, by [Serre3, p. 32, Prop. 21(c)], the residue fields of E, F_1, F_2, F at w coincide with the residue fields of E', F'_1, F'_2, F' at w', respectively.

We may therefore replace E, F_1, F_2, F, respectively, by E', F'_1, F'_2, F', if necessary, to assume that $w|_{F_1}$ is the unique extension of v to F_1. Now put $w_i = w|_{F_i}$, $i = 1, 2$. By Proposition 2.4.1, O_{w_1} is the integral closure of O_v in F_1. Since v is unramified in F_1, Proposition 2.3.2 implies $[F_1 : E] = [\bar{F}_1 : \bar{E}]$, where the bar denotes reduction modulo w.

Choose $x \in O_{w_1}$ such that $\bar{x}$ is a primitive element for the separable extension $\bar{F}_1/\bar{E}$. Let $f = \mathrm{irr}(x, E)$ and $p = \mathrm{irr}(\bar{x}, \bar{E})$. Then $f \in O_v[X]$ and $f(x) = 0$. Hence, $\bar{f}(\bar{x}) = 0$ and $p|\bar{f}$. Therefore,

$$[F_1 : E] \geq \deg(f) \geq \deg(\bar{p}) = [\bar{F}_1 : \bar{E}] = [F_1 : E].$$

Consequently, $p = \bar{f}$, $F_1 = E(x)$, and $\bar{F}_1 = \bar{E}(\bar{x})$.

By Lemma 2.3.6, w_2 is unramified in F. Thus, we may apply the result of the preceding paragraph to F/F_2 and conclude that $\bar{F} = \bar{F}_2(\bar{x})$. Consequently, $\bar{F}_1\bar{F}_2 = \bar{E}(\bar{x})\bar{F}_2 = \bar{F}_2(\bar{x}) = \bar{F}$. □

2.5 Linear Disjointness of Fields

Central to field theory is the concept "linear disjointness of fields", an analog of linear independence of vectors.

We repeat the convention made in "Notation and Convention" that whenever we form the compositum of fields, we tacitly assume they are contained in a common field.

LEMMA 2.5.1: *Let E and F be extensions of a field K. The following conditions are equivalent:*

(a) *Each m-tuple $(x_1, \ldots, x_m)$ of elements of E which is linearly independent over K is also linearly independent over F.*

(b) *Each n-tuple $(y_1, \ldots, y_n)$ of elements of F which is linearly independent over K is also linearly independent over E.*

Proof: It suffices to prove that (a) implies (b). Let $y_1, \ldots, y_n$ be elements of F for which there exist $a_1, \ldots, a_n \in E$ with $a_1y_1 + \cdots + a_ny_n = 0$. Let $\{x_j \mid j \in J\}$ be a linear basis for E over K and write $a_i = \sum_{j\in J} a_{ij}x_j$ with a_{ij} elements of K, only finitely many different from 0. Then

$$\sum_{j\in J} \Big(\sum_{i=1}^{n} a_{ij}y_i\Big)x_j = 0.$$

By (a), $\{x_j \mid j \in J\}$ is linearly independent over F. Hence, $\sum a_{ij}y_i = 0$ for every j. If $y_1, \ldots, y_m$ are linearly independent over K, then $a_{ij} = 0$ for every i and j, so $a_i = 0$, $i = 1, \ldots, m$. Thus, $y_1, \ldots, y_m$ are linearly independent over E. This proves (b). □

Definition: With E and F field extensions of a field K, refer to E and F as **linearly disjoint over** K if (a) (or (b)) of Lemma 2.5.1 holds. □

COROLLARY 2.5.2: *Let E and F be extensions of a field K such that $[E : K] < \infty$. Then E and F are linearly disjoint over K if and only if $[E : K] = [EF : F]$. If in addition $[F : K] < \infty$, then this is equivalent to $[EF : K] = [E : K][F : K]$.*

Proof: If E and F are linearly disjoint over K and $w_1, \ldots, w_n$ is a basis for E/K, then $w_1, \ldots, w_n$ is also a basis for EF over F. Hence, $[EF : F] = n = [E : K]$. Conversely, suppose $[E : K] = [EF : F]$ and let $x_1, \ldots, x_m \in E$ be linearly independent over K. Extend $\{x_1, \ldots, x_m\}$ to a basis $\{x_1, \ldots, x_n\}$ of E/K. Since $\{x_1, \ldots, x_n\}$ generates EF over F and $n = [EF : F]$, $\{x_1, \ldots, x_n\}$ is a basis of EF/F. In particular, $x_1, \ldots, x_m$ are linearly independent over F. □

Let E/K be a finite Galois extension. If $E \cap F = K$, then, by Corollary 2.5.2, E and F are linearly disjoint over K. The condition, $E \cap F = K$ is equivalent to "res: $\mathrm{Gal}(EF/F) \to \mathrm{Gal}(E/K)$ is an isomorphism" and also to "res: $\mathrm{Gal}(F) \to \mathrm{Gal}(E/K)$ is surjective." For arbitrary extensions this condition is clearly necessary, but not sufficient. Let L be a degree $n > 1$ extension of K for which L' is conjugate to L over K and $L' \cap L = K$. Then $[LL' : K] \leq n(n-1)$. Thus, according to Corollary 2.5.2, L and L' are not linearly disjoint over K. For example, $\mathbb{Q}(\sqrt[3]{2})$ is not linearly disjoint from $\mathbb{Q}(\zeta_3 \sqrt[3]{2})$ over $\mathbb{Q}$ although their intersection is $\mathbb{Q}$.

LEMMA 2.5.3 (Tower Property): *Let $K \subseteq E$ and $K \subseteq L \subseteq F$ be four fields. Then E is linearly disjoint from F over K if and only if E is linearly disjoint from L over K and EL is linearly disjoint from F over L.*

Proof: The only nontrivial part is to show that if E and F are linearly disjoint over K, then EL and F are linearly disjoint over L.

Apply Lemma 2.5.1. Suppose that $y_1, \ldots, y_m$ are elements of F which are linearly independent over L, but $a_1, \ldots, a_m$ are elements of EL such that $\sum_{i=1}^{m} a_i y_i = 0$. Clear denominators to assume that $a_i \in L[E]$, so that $a_i = \sum a_{ij} x_j$ with $a_{ij} \in L$, where $\{x_j \mid j \in J\}$ is a linear basis for E over K. Then $\sum_j (\sum_i a_{ij} y_i) x_j = 0$. By assumption, the x_j are linearly independent over F. Hence, $\sum_j a_{ij} y_i = 0$, so $a_{ij} = 0$ for all i and j. Consequently, $a_i = 0$, $i = 1, \ldots, m$. □

LEMMA 2.5.4: *Let L be a separable algebraic extension of a field K and let M be a purely inseparable extension of K. Then L and M are linearly disjoint over K.*

Proof: Let $\hat{L}$ be the Galois closure of L/K. Then $\hat{L} \cap M = K$. Hence, $\hat{L}$ and M are linearly disjoint over K. Therefore, by Lemma 2.5.3, L and M are linearly disjoint over K. □

Let $E_1, \ldots, E_n$ be n extensions of a field K. We say that $E_1, \ldots, E_n$ are **linearly disjoint** over K if $E_1 \cdots E_{m-1}$ and E_m are linearly disjoint over K for $m = 2, \ldots, n$. Induction on n shows that this is the case if and only if the following condition holds: If w_{i,j_i}, $j_i \in J_i$, are elements of E_i which are linearly independent over K, $i = 1, \ldots, n$, then $\prod_{i=1}^{n} w_{i,j_i}$, $(j_1, \ldots, j_n) \in J_1 \times \cdots \times J_n$, are linearly independent over K.

It follows that $E_1, \ldots, E_n$ are linearly disjoint over K if and only if the canonical homomorphism of $E_1 \otimes_K \cdots \otimes_K E_n$ into $E_1 \cdots E_n$ that maps $x_1 \otimes \cdots \otimes x_n$ onto $x_1 \cdots x_n$ is injective. It also follows that if $E_1, \ldots, E_n$ are linearly disjoint over K, then $E_{\pi(1)}, \ldots, E_{\pi(n)}$ are linearly disjoint over K for every permutation π of $\{1, \ldots, n\}$.

The application of tensor products makes the following lemma an easy observation.

LEMMA 2.5.5: *Let $E_1, \ldots, E_n$ (resp. $F_1, \ldots, F_n$) be linearly disjoint field extensions of K (resp. L). For each i between 1 and n let φ_i: $E_i \to F_i \cup \{\infty\}$,*

be either a place or an embedding. Suppose $\varphi_1, \dots, \varphi_n$ *coincide on* K *and* $\varphi_i(K) = L$, $i = 1, \dots, n$. *Let* $E = E_1 \cdots E_n$ *and* $F = F_1 \cdots F_n$. *Then there exists a place* $\varphi\colon E \to \tilde{F} \cup \{\infty\}$ *that extends each of the* φ_i*'s. If each* φ_i *is an isomorphism of* E_i *onto* F_i, *then* φ *is an isomorphism of* E *onto* F.

Proof: Let O_i be the valuation ring of φ_i if φ_i is a place and E_i if φ_i is an isomorphism. By assumption, the map $x_1 \cdots x_n \to x_1 \otimes \cdots \otimes x_n$ is an isomorphism $O_1 \cdots O_n \cong O_1 \otimes_K \cdots \otimes_K O_n$ of rings. Hence, there exists a ring homomorphism $\varphi_0\colon O_1 \cdots O_n \to F$ such that $\varphi_0(x) = \varphi_i(x)$ for each $x \in O_i$, $i = 1, \dots, n$. Extend φ_0 to a place $\varphi\colon E \to \tilde{F} \cup \{\infty\}$ (Proposition 2.3.1). If $x \in E_i \smallsetminus O_i$, then $\varphi(x^{-1}) = \varphi_i(x^{-1}) = 0$, so $\varphi(x) = \varphi_i(x) = \infty$. We conclude that φ coincides with φ_i on E_i. □

Finally, define a family $\{E_i \mid i \in I\}$ of field extensions of K to be **linearly disjoint over** K if every finite subfamily is linearly disjoint over K. It follows from the discussion preceding Lemma 2.5.5 that a sequence $(E_1, E_2, E_3, \dots)$ of fields extensions of K is linearly disjoint over K if E_n is linearly disjoint from $E_1 \cdots E_{n-1}$ for $2, 3, 4, \dots$. Then, $E_{\pi(1)}, E_{\pi(2)}, E_{\pi(3)}, \dots$ are linearly disjoint for every permutation π of $\mathbb{N}$.

LEMMA 2.5.6: *Let* $\{L_i \mid i \in I\}$ *be a linearly disjoint family of Galois extensions of a field* K. *Then* $\operatorname{Gal}(\prod_{i\in I} L_i/K) \cong \prod_{i\in I} \operatorname{Gal}(L_i/K)$.

Proof: Since $\prod_{i\in I} \operatorname{Gal}(L_i/K) \cong \varprojlim \prod_{i\in I_0} \operatorname{Gal}(L_i/K)$, we may assume I is finite. In this case, the embedding $\operatorname{Gal}(\prod_{i\in I} L_i/K) \to \prod_{i\in I} \operatorname{Gal}(L_i/K)$ given by $\sigma \mapsto (\sigma|_{L_i})_{i\in I}$ is surjective (Lemma 2.5.5). Therefore, it is an isomorphism. □

LEMMA 2.5.7: *Let* K *be a field,* $K_1, K_2, K_3, \dots$ *a linearly disjoint sequence of extensions of* K, *and* L *a finite separable extension of* K. *Then there exists a positive integer* n *such that* $L, K_n, K_{n+1}, K_{n+2}, \dots$ *are linearly disjoint over* K.

Proof: Replace L by its Galois closure over K, if necessary, to assume L is Galois over K. Assume for each positive integer n the field L is not linearly disjoint from $K_n K_{n+1} K_{n+2} \cdots$ over K. Then $L_n = L \cap K_n K_{n+1} K_{n+2} \cdots$ is a proper extension of K. Since L has only finitely many extensions that contain K and since $L_n \supseteq L_{n+1} \supseteq L_{n+2} \supseteq \cdots$, there is an m such that $L_n = L_m$ for all $n \geq m$. Since L_m is a finite extension of K, there is an $n > m$ with $L_m \subseteq K_m \cdots K_{n-1}$. Similarly, there exists $r > n$ with $L_m \subseteq K_n \cdots K_{r-1}$. By assumption, $K_m \cdots K_{n-1}$ and $K_n \cdots K_{r-1}$ are linearly disjoint over K. In particular, their intersection is K. Therefore, $L_m = K$. This contradiction proves there exists n such that $L, K_n, K_{n+1}, K_{n+2}, \dots$ are linearly disjoint over K. □

LEMMA 2.5.8: *Let* v *be a discrete valuation of a field* K *and* L, M *finite extensions of* K. *Suppose* v *is unramified in* L *but totally ramified in* M. *Then* L *and* M *are linearly disjoint over* K.

Proof: Let L_0 be the maximal separable extension of K in L and v_0 an extension of v to L_0. Then L/L_0 is purely inseparable. Hence, v_0 is ramified in L. Therefore, $L = L_0$ and L/K is separable.

Since v is unramified in each of the conjugates of L over K, it is unramified in their compositum (Corollary 2.3.7). We may therefore replace L by the Galois closure of L/K, if necessary, to assume L/K is Galois.

Let $m = [L \cap M : K]$. Choose an extension w of v to $L \cap M$. Then $e(w/v) = 1$ on one hand and $e(w/v) = m$ on the other hand. Thus, $L \cap M = K$. Therefore, L is linearly disjoint from M over K. □

Example 2.5.9: Roots of unity. For each n consider the Galois extension $\mathbb{Q}(\zeta_n)$ of $\mathbb{Q}$ obtained by adjoining a primitive root of unity of order n. It is well known that $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ is the number of integers between 1 and n which are relatively prime to n [Lang7, p. 278, Thm. 3.1]. If m is relatively prime to n, then $\varphi(mn) = \varphi(m)\varphi(n)$ [LeVeque, p. 28, Thm. 3-7]. In addition, $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn})$. Hence, $[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] = \varphi(mn) = \varphi(m)\varphi(n) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}][\mathbb{Q}(\zeta_n) : \mathbb{Q}]$. It follows from Corollary 2.5.2 that $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_n)$ are linearly disjoint over $\mathbb{Q}$. □

Here is an application of linear disjointness to integral closures of domains.

LEMMA 2.5.10: *Let K be a field, L a separable algebraic extension of K, and R an integrally closed integral domain containing K. Let $E = \mathrm{Quot}(R)$, $F = EL$, and S the integral closure of R in F. Suppose E and L are linearly disjoint over K. Then $S = RL \cong R \otimes_K L$.*

Proof: Assume without loss L/K is finite. Choose a basis $w_1, \ldots, w_n$ for L/K. Let $\sigma_1, \ldots, \sigma_n$ be the distinct K-embeddings of L into K_s. Then $\det(\sigma_i w_j) \neq 0$.

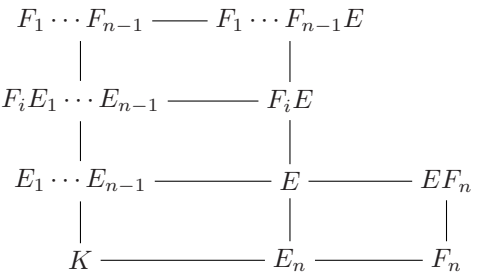
Each element of L is integral over K, hence over R, so $RL \subseteq S$. Conversely, let $x \in S$. By the linear disjointness, $w_1, \ldots, w_n$ form a basis for F/E. Hence, $x = \sum_{j=1}^n e_j w_j$ with $e_j \in E$, $j = 1, \ldots, n$. Also, each σ_i extends to an E-embedding of F into E_s (Lemma 2.5.5). Thus, $\sigma_i x = \sum_{j=1}^n e_j \sigma_i w_j$, $i = 1, \ldots, n$. Apply Kramer's law to present each e_k as a polynomial in $\sigma_i x, \sigma_i w_j$, with $i, j = 1, \ldots, n$, divided by $\det(\sigma_i w_j)$. Thus, e_k is an element of E which is integral over R. Since R is integrally closed, $e_k \in R$, $k = 1, \ldots, n$. Consequently, $x \in RL$, as needed. □

We generalize the tower property to families of field extensions:

LEMMA 2.5.11: *Let K be a field and I a set. For each $i \in I$ let F_i/E_i be a field extension with $K \subseteq E_i$. Suppose $\{F_i \mid i \in I\}$ is linearly disjoint over K. Denote the compositum of all E_i's by E. Then the set $\{F_i E \mid i \in I\}$ is linearly disjoint over E. Moreover, for each $i \in I$, the field F_i is linearly disjoint from E over E_i.*

Proof: It suffices to consider the case where $I = \{1, 2, \ldots, n\}$. By induction suppose $F_i E_1 \cdots E_{n-1}$, $i = 1, \ldots, n-1$, are linearly disjoint over $E_1 \cdots E_n$.

By assumption, $F_1 \cdots F_{n-1}$ is linearly disjoint from F_n over K. Hence, by the tower property, $F_1 \cdots F_{n-1}$ is linearly disjoint from E over $E_1, \ldots, E_{n-1}$, so $F_i E$, $i = 1, \ldots, n-1$, are linearly disjoint over E.



Moreover, $F_1 \cdots F_{n-1}E$ is linearly disjoint from EF_n over E. Consequently, E is linearly disjoint from F_n over E_n and F_iE, $i = 1, \ldots, n$ are linearly disjoint over E, as claimed. □

2.6 Separable, Regular, and Primary Extensions

Based on the notion of linear disjointness we define here three type of field extensions. We say that a field extension F/K is **separable** (resp. **regular, primary**) if F is linearly disjoint from K_{ins} (resp. $\tilde{K}$, K_s) over K.

Separable Extensions. We generalize the notion of "separable algebraic extension" to arbitrary field extensions.

Let K be a field of positive characteristic p. The field generated over K by the pth roots of all elements of K is denoted $K^{1/p}$. We denote the maximal purely inseparable extension of K by K_{ins} (or K^{1/p^∞}). Let F be a finitely generated extension of K. A collection $t_1, \ldots, t_r \in F$ of elements algebraically independent over K is a **separating transcendence basis** if $F/K(t_1, \ldots, t_r)$ is a finite separable extension.

Lemma 2.6.1: *An extension F of a field K is separable if it satisfies one of the following equivalent conditions:*
(a) *F is linearly disjoint from K_{ins} over K.*
(b) *F is linearly disjoint from $K^{1/p}$ over K.*
(c) *Every finitely generated extension E of K which is contained in F has a separating transcendence basis.*

Moreover, a separating transcendence basis can be selected from a given set of generators for F/K.

Proof: The implications "(a) => (b)" and "(c) => (a)" are immediate consequences of the tower property (Lemma 2.5.3). For "(b) => (c)" see [Lang 4, p. 54]. Lemma 19.2.4 gives a constructive proof. □

In particular, every separable algebraic extension satisfies conditions (a), (b), and (c) of Lemma 2.6.1. Now apply the rules of linear disjointness.

COROLLARY 2.6.2:
(a) *If E/K and F/E are separable extensions, then F/K is also separable.*
(b) *If F/K is a separable extension, then E/K is separable for every field $K \subseteq E \subseteq F$.*
(c) *Every extension of a perfect field is separable.*
(d) *If E/K is a purely inseparable extension and F/K is a separable extension, then E and F are linearly disjoint over K.*

Example 2.6.3: A separable tower does not imply separable steps. Consider the tower of fields $\mathbb{F}_p \subset \mathbb{F}_p(t^p) \subset \mathbb{F}_p(t)$, where t is transcendental over $\mathbb{F}_p$. The extension $\mathbb{F}_p(t)/\mathbb{F}_p$ is separable, but $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ is not. □

REGULAR EXTENSIONS. Finitely generated regular extensions characterize absolutely irreducible varieties (Section 10.2)

LEMMA 2.6.4: *A field extension F/K is regular if it satisfies one of the following equivalent conditions:*
(a) *F/K is separable and K is algebraically closed in F.*
(b) *F is linearly disjoint from $\tilde{K}$ over K.*

Proof: The implication "(b) => (a)" is immediate.

To prove "(a) => (b)", it suffices to assume that F/K is finitely generated. Then F/K has a separating transcendence basis, $t_1, \ldots, t_r$, which is also a separating transcendence basis for the extension FK_s/K_s. Since $\tilde{K} = (K_s)_{\text{ins}}$, Lemma 2.6.1 implies that FK_s is linearly disjoint from $\tilde{K}$ over K_s. Also, K_s/K is a Galois extension and $F \cap K_s = K$. Hence, F is linearly disjoint from K_s over K. Therefore, by Lemma 2.5.3, F is linearly disjoint from $\tilde{K}$ over K. □

COROLLARY 2.6.5:
(a) *If E/K and F/E are regular extensions, then F/K is regular.*
(b) *If F/K is a regular extension, then E/K is regular for every field E lying between K and F.*
(c) *Every extension of an algebraically closed field is regular.*
(d) *Let m be a cardinal number and K_α, $\alpha \leq m$, an ascending transfinite sequence of fields such that $K_\gamma = \bigcup_{\alpha<\gamma} K_\alpha$ for each limit ordinal number $\gamma \leq m$. Suppose $K_{\gamma+1}$ is a regular extension of K_γ for all $\gamma < m$. Then K_m is a regular extension of each K_β with $\beta < m$.*

Proof of (d): Let $\delta \leq m$ be a transfinite number. By transfinite induction assume K_γ is regular extension of K_β for all $\beta \leq \gamma < \delta$. Now distinguish between two cases:

CASE A: *δ is a limit number.* Consider $\beta < \delta$, elements $a_1, \ldots, a_r \in \tilde{K}_\beta$ linearly independent over K_β, and elements $u_1, \ldots, u_r \in K_\delta$ satisfying $\sum_{i=1}^r a_i u_i = 0$. Then there exists an ordinal number γ with $\beta \leq \gamma < \delta$ and $u_1, \ldots, u_r \in K_\gamma$. Since K_γ/K_β is regular, $\tilde{K}_\beta$ is linearly disjoint from K_γ

over K_β, so $a_1 = \cdots = a_r = 0$. Therefore, K_δ is linearly disjoint from $\tilde{K}_\beta$ over K_β.

CASE B: $\delta = \gamma + 1$ *is a successor number.* By assumption, both K_γ/K_β and $K_{\gamma+1}/K_\gamma$ are regular extensions. Hence, by (a), K_δ/K_β is a regular extension. □

The next lemma gives a criterion for a regular extension F/K to be linearly disjoint from another extension of K in terms of "algebraic independence". To define this notion consider an arbitrary field extension F/K and a subset T of F. We say that T is **algebraically independent** over K if $f(t_1, \ldots, t_n) \neq 0$ for all $t_1, \ldots, t_n \in T$ and for each nonzero $f \in K[X_1, \ldots, X_n]$. If in addition $F/K(T)$ is an algebraic extension, then T is a **transcendence base** of F/K. The cardinality of T depends only on F/K. It is the **transcendence degree** of F/K. We denote it by trans.deg(F/K). For example, trans.deg$(F/K) = 0$ if and only if F/K is an algebraic extension. If S is a subset of F such that $F/K(S)$ is algebraic, then S contains a transcendence base for F/K [Lang7, p. 356, Thm. 1.1]. In particular, if F/K is finitely generated, then trans.deg$(F/K) < \infty$. The converse is false. For example, trans.deg$(\tilde{\mathbb{Q}}/\mathbb{Q}) = 0$ although $\tilde{\mathbb{Q}}/\mathbb{Q}$ is not finitely generated.

If T_0 is a subset of F which is algebraically independent over K, choose a transcendence base T_1 for $F/K(T_0)$. Then $T_0 \cap T_1 = \emptyset$ and $T_0 \cup T_1$ is a transcendence base for F/K. This argument also gives the additivity of the transcendence degree for a tower $K \subseteq E \subseteq F$ of fields:

$$\text{trans.deg}(F/K) = \text{trans.deg}(E/K) + \text{trans.deg}(F/E). \tag{1}$$

Now consider two extensions E and F of a field K. We say that E and F are **algebraically independent** over K if

(2) every m-tuple $(t_1, \ldots, t_m)$ of elements of E which is algebraically independent over K is also algebraically independent over F.

It follows that E and F are algebraically independent over K if and only if E_0 and F are algebraically independent over K for every subfield E_0 of E which is finitely generated over K. Hence, in order to prove that algebraic independence is a symmetric relation, we may consider finitely generated extensions E and F of K, assume that (2) holds, and prove condition (2) with the roles of E and F exchanged. Indeed, let $u_1, \ldots, u_n$ be elements of F which are algebraically independent over K. Enlarge n, if necessary, to assume that $u_1, \ldots, u_n$ form a transcendence base of F/K. Then $F/K(\mathbf{u})$ is algebraic and therefore so is $EF/E(\mathbf{u})$. After reordering the u_i, we may assume $u_1, \ldots, u_m$ form a transcendence base for EF/E. Assumption (2) implies that trans.deg(E/K) = trans.deg(EF/F). Hence, by (1), m = trans.deg(EF/E) = trans.deg(EF/K) − trans.deg(E/K) = trans.deg(EF/K) − trans.deg(EF/F) = trans.deg$(F/K) = n$. Therefore, $u_1, \ldots, u_n$ are algebraically independent over E, as desired.

Like linear disjointness, algebraic independence has the tower property: Let $K \subseteq L \subseteq M$ and $K' \subseteq L' \subseteq M'$ be fields with $K \subseteq K'$, $L' = K'L$ and

$M' = L'M$. Then trans.deg(M/K) = trans.deg(L/K)+trans.deg(M/L) and trans.deg(M'/K') = trans.deg(L'/K') + trans.deg(M'/L'). Also,

$$\text{trans.deg}(L'/K') \leq \text{trans.deg}(L/K),\ \ \text{trans.deg}(M'/L') \leq \text{trans.deg}(M/L).$$

Hence, M is algebraically independent from K' over K if and only if L is algebraically independent from K' over K and M is algebraically independent from L' over L.

By considering monomials in elements $x_1, \ldots, x_n$ of E, it is clear that if E and F are linearly disjoint over K, then they are also algebraically independent over K. The converse, however, is false: Any two extensions of K one of which is algebraic are algebraically independent over K. Lemma 2.6.7 below gives a partial converse.

LEMMA 2.6.6: *Let F and $\bar{F}$ be fields, T (resp. $\bar{T}$) an algebraically independent set over F (resp. over $\bar{F}$), $\varphi_0\colon F \to \bar{F} \cup \{\infty\}$ a place, and $\varphi_1\colon T \to \bar{T}$ a bijective map. Then there exists a place $\varphi\colon F(T) \to \bar{F}(\bar{T}) \cup \{\infty\}$ extending both φ_0 and φ_1.*

Proof: The case where T consists of one element t is covered by Example 2.3.3. In the general case well order T and apply transfinite induction. □

LEMMA 2.6.7: *Let E be a regular extension of a field K and let F be an extension of K. If E and F are algebraically independent over K, then E and F are linearly disjoint over K.*

Proof (Artin): Let $x_1, \ldots, x_n$ be elements of E for which there exist $a_1, \ldots, a_n \in F$, not all zero, such that $\sum a_i x_i = 0$. Use Proposition 2.3.1 to choose a K-place φ of F into $\tilde{K} \cup \{\infty\}$. Let T be a transcendence base for E over K. Then the elements of T are algebraically independent over F. Hence, by Lemma 2.6.6, φ extends to a $K(T)$-place of $F(T)$. Since E is an algebraic extension of $K(T)$, φ extends to an E-place of EF into $\tilde{E} \cup \{\infty\}$ (Lemma 2.4.2).

With no loss we may divide $a_1, \ldots, a_n$ by, say a_1, to assume that $a_1 = 1$ and that all the a_i are finite under φ. Thus, $\sum \varphi(a_i) x_i = 0$ is a nontrivial linear combination of the x_i over $\tilde{K}$. But E is linearly disjoint from $\tilde{K}$ over K. Hence, $x_1, \ldots, x_n$ are also linearly dependent over K. □

COROLLARY 2.6.8:

(a) *Let E be a regular extension of a field K, algebraically independent from an extension F of K. Then EF is a regular extension of F.*

(b) *If two regular extensions E and F of K are algebraically independent, then EF/K is regular.*

Proof: For (a) note that E is also algebraically independent from $\tilde{F}$ over K. By Lemma 2.6.7, E is linearly disjoint from $\tilde{F}$ over K. Hence, by Lemma 2.5.3, EF is linearly disjoint from $\tilde{F}$ over F. Therefore, EF/F is regular.

For (b) use (a) and Corollary 2.6.5(a). □

LEMMA 2.6.9: *Each of the following conditions on a field extension F/K implies that F/K is regular:*

(a) *For all $u_1, \dots, u_n \in F^\times$, there exists a K-place $\varphi\colon F \to \tilde{K} \cup \{\infty\}$ with $\varphi(u_1), \dots, \varphi(u_n) \in K^\times$.*

(b) *There exists a K-place $\varphi\colon F \to K \cup \{\infty\}$.*

Proof: We prove that F/K satisfies Condition (b) of Lemma 2.6.4. Consider $w_1, \dots, w_n$ in $\tilde{K}$ which are linearly independent over K. Assume there exist $u_1, \dots, u_n$ in F, not all zero, such that $\sum_{i=1}^n u_i w_i = 0$. Omitting the terms with $u_i = 0$, we may assume $u_i \neq 0$ for all i. In Case (a) choose a K-place $\varphi\colon F \to \tilde{K} \cup \{\infty\}$ with $\varphi(u_i) \in K^\times$ for each i such that $u_i \neq 0$. In Case (b) divide $u_1, \dots, u_n$ with one of them, say with u_1, to assume that $u_1 = 1$ and that $\varphi(u_i) \in K$ for $i = 1, \dots, n$. Now apply Proposition 2.3.1 and extend φ to a place $\tilde{\varphi}\colon F\tilde{K} \to \tilde{K} \cup \{\infty\}$. By Lemma 2.4.2, $\tilde{\varphi}$ is trivial on $\tilde{K}$. In other words, the restriction of $\tilde{\varphi}$ to $\tilde{K}$ is an automorphism.

In particular, $\tilde{\varphi}(w_1), \dots, \tilde{\varphi}(w_n)$ are linearly independent over K. Since $\sum_{i=1}^n \varphi(u_i)\tilde{\varphi}(w_i) = 0$, this implies $\varphi(u_i) = 0$ for $i = 1, \dots, n$. This contradiction proves that $w_1, \dots, w_n$ are linearly independent over F. We conclude that F is linearly disjoint from K over $\tilde{K}$. $\square$

Example 2.6.10: Purely transcendental extensions. Let $t_1, \dots, t_n$ be algebraically independent elements over a field K. For each i between 1 and n the map $t_i \to 0$ extends to a $K(t_1, \dots, t_{i-1})$-place φ_i of $K(t_1, \dots, t_i)$ onto $K(t_1, \dots, t_{i-1}) \cup \{\infty\}$. Hence, by Lemma 2.6.9(b),

$$K(t_1, \dots, t_i)/K(t_1, \dots, t_{i-1})$$

is a regular extension. Therefore, by Corollary 2.6.9(a), $K(\mathbf{t})/K$ is a regular extension.

Of course, we can also prove the latter result directly: Let $f_1, \dots, f_m$ be elements of $K(\mathbf{t})$ which are linearly dependent over $\tilde{K}$. Thus, there are $\tilde{c}_1, \dots, \tilde{c}_m \in \tilde{K}$ not all zero with $\sum_{i=0}^m \tilde{c}_i f_i = 0$. Clearing denominators, we may assume all $f_i \in K[\mathbf{t}]$. Write $f_i(\mathbf{t}) = \sum_{\mathbf{j}} a_{i\mathbf{j}} t_1^{j_1} \cdots t_n^{j_n}$. Then $\sum_{\mathbf{j}} \big(\sum_{i=1}^m \tilde{c}_i a_{i\mathbf{j}} \big) t_1^{j_1} \cdots t_n^{j_n} = \sum_{i=1}^m \tilde{c}_i f_i(\mathbf{t}) = 0$. Hence, $\sum_{i=1}^m \tilde{c}_i a_{i\mathbf{j}} = 0$ for all $\mathbf{j}$. Thus, the homogeneous linear system of equations $\sum_{i=1}^m X_i a_{i\mathbf{j}} = 0$ with coefficients $\mathbf{a}_{i\mathbf{j}} \in K$ has a nonzero solution in $\tilde{K}^n$. Therefore, it has a nonzero solution in K^n. In other words, there are $c_1, \dots, c_n \in K$ not all zero with $\sum_{i=1}^m c_i a_{i\mathbf{j}} = 0$ for all $\mathbf{j}$. They satisfy $\sum_{i=1}^m c_i f_i = 0$. Hence, $f_1, \dots, f_m$ are linearly dependent over K. This completes the direct proof that $K(\mathbf{t})/K$ is a regular extension.

We have not defined composition of places. But if we had, we could compose the places $\varphi_i\colon K(t_1, \dots, t_i) \to K(t_1, \dots, t_{i-1})$, $i = n, n-1, \dots, 1$, of the first paragraph to a K-place $\varphi\colon K(\mathbf{t}) \to K$ satisfying $\varphi(t_i) = 0$, $i = 1, \dots, n$. Again, by Lemma 2.6.9(b), this would prove that $K(\mathbf{t})/K$ is regular. Also, given $a_1, \dots, a_n \in K$, we can replace t_i by $t_i - a_i$ to produce a K-place $\psi\colon K(\mathbf{t}) \to K$ with $\psi(t_i) = a_i$, $i = 1, \dots, n$.

Let now T be an arbitrary set of algebraically independent elements over K and $\varphi_0\colon T \to K$ a map. Then every finitely generated subextension of $K(T)/K$ is regular. Therefore, $K(T)/K$ is regular. Moreover, using transfinite induction, it is possible to construct a K-place $\varphi\colon K(T) \to K$ which extends φ_0. □

Example 2.6.11: Absolutely irreducible polynomials. Now consider a polynomial $f \in K[T_1, \ldots, T_n, X]$. Suppose f is **absolutely irreducible**; that is, f is irreducible in $\tilde{K}[T_1, \ldots, T_n, X]$. Let x be a root of $f(\mathbf{t}, X)$ in $\widetilde{K(\mathbf{t})}$. Then $[K(\mathbf{t}, x) : K(\mathbf{t})] = \deg_X f = [\tilde{K}(\mathbf{t}, x) : \tilde{K}(\mathbf{t})]$. By Corollary 2.5.2, $K(\mathbf{t}, x)$ is linearly disjoint from $\tilde{K}(\mathbf{t})$ over $K(\mathbf{t})$. By Example 2.6.10, $K(\mathbf{t})$ is linearly disjoint from $\tilde{K}$ over K. Hence, by the tower property (Lemma 2.5.3), $K(\mathbf{t}, x)$ is linearly disjoint from $\tilde{K}$ over K. Therefore, $K(\mathbf{t}, x)/K$ is a regular extension.

Conversely, suppose f is irreducible in $K[\mathbf{T}, X]$ and $K(\mathbf{t}, x)/K$ is a regular extension. Reversing the above arguments shows that f is absolutely irreducible. □

As an application we rephrase Corollary 1.3.4 and supply a new proof. It is a simplified version of [Leptin].

Proposition 2.6.12: *Let G be a profinite group and K a field. Then there is a Galois extension F/E with $K \subseteq E$ and* $\mathrm{Gal}(F/E) \cong G$.

Proof: Write G as a projective limit $\varprojlim G_i$ of finite groups G_i with i ranging over a directed set I. By definition, G is a closed subgroup of $\prod_{i\in I} G_i$. Suppose we have constructed an algebraic extension F/E with $K \subseteq E$ and $\mathrm{Gal}(F/E) \cong \prod_{i\in I} G_i$. Let E' be the fixed field of G in F. Then $\mathrm{Gal}(F/E') \cong G$.

In order to construct F/E with $\mathrm{Gal}(F/E) \cong \prod_{i\in I} G_i$, we choose a family $(x_i^\sigma)_{i\in I,\, \sigma\in G_i}$ of algebraically independent elements over K. For each $i \in I$ let $F_i = K(x_i^\sigma \mid \sigma \in G_i)$. The group G_i acts on F_i by the rule $(x_i^\sigma)^\tau = x_i^{\sigma\tau}$ and $a^\tau = a$ for $a \in K$. Let E_i be the fixed field. Then $K \subseteq E_i$ and F_i/E_i is a Galois extension with Galois group G_i [Lang7, p. 264].

Denote the compositum of all E_i's by E and the compositum of all F_i's by F. By Example 2.6.10, each F_i is a regular extension of K. By construction, the set $\{F_i \mid i \in I\}$ is algebraically independent over K. Hence, by Lemma 2.6.7, the set $\{F_i \mid i \in I\}$ is linearly disjoint over K. It follows from Lemma 2.5.11, that the set $\{EF_i \mid i \in I\}$ is linearly disjoint over E. Moreover, E is linearly disjoint from F_i over E_i. Therefore, $\mathrm{Gal}(EF_i/E) \cong \mathrm{Gal}(F_i/E_i) \cong G_i$. It follows from Lemma 2.5.6 that $\mathrm{Gal}(F/E) \cong \prod_{i\in I} G_i$, as desired. □

Primary Extensions. We use primary extensions in the study of C_i-fields (Section 21.2).

Lemma 2.6.13: *A field extension F/K is primary if it satisfies one of the following equivalent conditions:*

(a) *$F \cap \tilde{K}/K$ is a purely inseparable extension.*
(b) *The field F is linearly disjoint from K_s over K.*

Proof: Clearly "(b) => (a)." The implication "(a) => (b)" holds since $F \cap K_s = K$ and K_s/K is a Galois extension. □

Corollary 2.6.14:
(a) *If E/K and F/E are primary extensions, then so is F/K.*
(b) *If F/K is a primary extension, then E/K is primary, for every field $K \subseteq E \subseteq F$.*
(c) *Every extension of a separably closed field is primary.*
(d) *An extension F/K is regular if and only if it is separable and primary.*

Lemma 2.6.15:
(a) *Let E be a primary extension of a field K which is algebraically independent from an extension F of K. Then EF is a primary extension of F.*
(b) *If two primary extensions E and F of K are algebraically independent, then EF/K is primary.*

Proof: Assertion (b) follows from (a) and from Corollary 2.6.14(a). To prove (a), choose a transcendence base T for E/K and let M be the maximal separable extension of $K(T)$ in E. Then M is a separable and primary extension of K. Hence, by Lemma 2.6.14(d), it is regular. Also, M is algebraically independent from F_s over K. By Lemma 2.6.7, MF is linearly disjoint from F_s over F. Since EF is a purely inseparable extension of MF, it is linearly disjoint from MF_s. It follows that EF is linearly disjoint from F_s over F; that is, EF is a primary extension of F. □

2.7 The Imperfect Degree of a Field

We classify fields of positive characteristic by their imperfect degree and characterize those fields for which every finite extension has a primitive element as fields of imperfect degree 1.

Let F be a field of positive characteristic p. Consider a subfield F_0 of F that contains the field F^p of all pth powers in F. Observe that for $x_1, \ldots, x_n \in F$, the set of monomials

$$x_1^{i_1} \cdots x_n^{i_n}, \qquad 0 \leq i_1, \ldots, i_n \leq p-1, \tag{1}$$

generates $F_0(\mathbf{x})$ over F_0. Hence, $[F_0(\mathbf{x}) : F_0] \leq p^n$. If $[F_0(\mathbf{x}) : F_0] = p^n$, then $x_1, \ldots, x_n$ are said to be **p-independent over F_0**. Equivalently, each of the fields $F_0(x_1), \ldots, F_0(x_n)$ has degree p over F_0 and they are linearly disjoint over F_0. This means that the set of monomials (1) is linearly independent over F_0. A subset B of F is **p-independent over F_0**, if every finite subset of B is p-independent over F_0. If in addition $F_0(B) = F$, then B is said to be a **p-basis** for F over F_0. As in the theory of vector spaces, each maximal p-independent subset of F over F_0 is a p-basis for F over F_0.

If $x_1, \ldots, x_n \in F$ are p-independent over F^p, we call them **p-independent** elements of F. The p-power $p^n = [F : F^p]$ is the **imperfect degree** of F and n is the **imperfect exponent** of F. We say that F is **n-imperfect**. Thus, a perfect field has imperfect exponent 0. Both quantities are **infinite** if $[F : F^p] = \infty$. In this case F is **∞-imperfect**.

LEMMA 2.7.1 (Exchange Principle): *Let F_0 be a subfield of F which contains F^p.*

(a) *Let $x_1, \ldots, x_m, y_1, \ldots, y_n \in F$ be such that $x_1, \ldots, x_m$ are p-independent over F_0 and $x_1, \ldots, x_m \in F_0(y_1, \ldots, y_n)$. Then $m \leq n$, and there is a reordering of $y_1, \ldots, y_n$ so that $y_1, \ldots, y_m \in F_0(x_1, \ldots, x_m, y_{m+1}, \ldots, y_n)$.*

(b) *Every subset of F which is p-independent over F_0 extends to a p-basis for F over F_0.*

Proof: We use induction on m. Assume the lemma is true for $m = k$. Thus, for $m = k + 1$ we may assume that

$$x_{k+1} \in F_0(x_1, \ldots, x_k, y_{k+1}, \ldots, y_n) = F_1.$$

Then $[F_1 : F_0] \leq p^n$ and there exists l between $k + 1$ and n such that

$$y_l \in F_0(x_1, \ldots, x_{k+1}, y_{k+1}, \ldots, y_{l-1}),$$

since otherwise $[F_1 : F_0] \geq p^{n+1}$, a contradiction. Thus, y_l can be exchanged for x_{k+1}. This proves the first part of the lemma for $m = k + 1$.

For the last part start from a subset A of K which is p-independent over F_0. Use Zorn's lemma to prove the existence of a maximal subset B of F which contains A and which is p-independent over F_0. Then B is a p-basis of F over F_0. □

LEMMA 2.7.2: *Suppose F is a finitely generated extension of transcendence degree n of a perfect field K of positive characteristic p. Then the imperfect exponent of F is n.*

Proof: Choose a separating transcendence basis $t_1, \ldots, t_n$ for F/K. Then $K(\mathbf{t})^p = K(\mathbf{t}^p)$ and $t_1, \ldots, t_n$ is a p-basis for $K(\mathbf{t})/K(\mathbf{t}^p)$; that is, $[K(\mathbf{t}) : K(\mathbf{t}^p)] = p^n$. Since $K(\mathbf{t})$ is a purely inseparable extension of $K(\mathbf{t}^p)$ and F^p is a separable extension of $K(\mathbf{t}^p)$, these extensions of $K(\mathbf{t}^p)$ are linearly disjoint. Also, F is both a separable extension and a purely inseparable extension of $K(\mathbf{t})F^p$. Hence, $F = K(\mathbf{t})F^p$. Consequently, $[F : F^p] = [K(\mathbf{t}) : K(\mathbf{t}^p)] = p^n$, as claimed. □

LEMMA 2.7.3: *Let B a subset of F which is p-independent over F^p and F' a separable extension of F. Then B is p-independent over $(F')^p$. If, in addition, F' is separable algebraic over F, then the imperfect degree of F' is equal to that of F.*

Proof: Assume without loss that B consists of n elements. Then $[(F')^p(B) : (F')^p] = [F^p(B) : F^p] = p^n$. Hence, B is p-independent over $(F')^p$.

Suppose now F'/F is separably algebraic. Then F' is both separably and purely inseparable over $F(F')^p$, so, $F' = F(F')^p$. Hence, $[F' : (F')^p] = [F : F^p]$. Therefore, the imperfect degree of F' is equal to that of F. □

LEMMA 2.7.4: *Let K be a field of positive characteristic p, let $a, b_1, \ldots, b_m$ be p-independent elements of K, and let $x_1, \ldots, x_m$ be algebraically independent over K. Suppose $y_1, \ldots, y_m$ satisfy*

$$ax_i^p + b_i y_i^p = 1, \quad i = 1, \ldots, m. \tag{2}$$

Then K is algebraically closed in $K(\mathbf{x}, \mathbf{y}) = K_m$.

Proof: We use induction on m.

PART A: $m = 1$. Let $x = x_1$, $y = y_1$, and $b = b_1$ and assume that u is a nonzero element of K_1 which is algebraic over K. Then u is also algebraic over $K(a^{1/p}, b^{1/p})$. But $K(x, y, a^{1/p}, b^{1/p}) = K(x, a^{1/p}, b^{1/p})$ is a purely transcendental extension of $K(a^{1/p}, b^{1/p})$. Hence, $u \in K(a^{1/p}, b^{1/p})$ and therefore $u^p \in K$. Write

$$u = \frac{h_0(x)}{h(x)} + \frac{h_1(x)}{h(x)} y + \cdots + \frac{h_k(x)}{h(x)} y^k \tag{3}$$

with $k \leq p-1$, $h(x), h_0(x), \ldots, h_k(x) \in K[x]$ and $h(x), h_k(x) \neq 0$. With no loss we may assume that x does not divide the greatest common divisor of $h(x), h_0(x), \ldots, h_k(x)$. Raise (3) to the pth power, multiply it by $h(x)^p$ and substitute $y^p = (1 - ax^p)b^{-1}$ to obtain:

$$(h(x)u)^p = h_0(x)^p + h_1(x)^p(1 - ax^p)b^{-1} + \cdots + h_k(x)^p(1 - ax^p)^k b^{-k}. \tag{4}$$

If $h(0) = 0$, then the substitution $x = 0$ in (4) gives

$$0 = h_0(0)^p + h_1(0)^p b^{-1} + \cdots + h_k(0)^p b^{-k},$$

Therefore, $h_0(0) = h_1(0) = \cdots = h_k(0) = 0$, contrary to assumption. Thus, we may assume $h(0) \neq 0$. Then the substitution $x = 0$ in (4) shows that $u \in K(b^{1/p})$. Similarly, $u \in K(a^{1/p})$. Since a and b are p-independent in K, $u \in K(a^{1/p}) \cap K(b^{1/p}) = K$.

Thus, K is algebraically closed in $K(x, y)$.

PART B: *Induction.* Assume the Lemma is true for $m - 1$. Then K is algebraically closed in $K_{m-1} = K(x_1, \ldots, x_{m-1}, y_1, \ldots, y_{m-1})$. If we prove that a and b_m are p-independent in K_{m-1}, then with K_{m-1} replacing K in Part A, K_{m-1} is algebraically closed in K_m, so K is algebraically closed in K_m.

Since $x_1, \ldots, x_m$ are algebraically independent over K, the field $K(a^{1/p}, b_1^{1/p}, \ldots, b_m^{1/p})$ is linearly disjoint from $E_{m-1} = K(x_1, \ldots, x_{m-1})$ over K. Thus,

$$[E_{m-1}(a^{1/p}, b_1^{1/p}, \ldots, b_m^{1/p}) : E_{m-1}] = p^{m+1}. \tag{5}$$

Also, from (2)

$$K_{m-1} = E_{m-1}(y_1, \ldots, y_{m-1}) \quad \text{and}$$
$$K_{m-1}(a^{1/p}, b_m^{1/p}) = E_{m-1}(a^{1/p}, b_1^{1/p}, \ldots, b_m^{1/p}).$$

Thus,

$$(6) \qquad [K_{m-1} : E_{m-1}] \leq p^{m-1} \quad \text{and} \quad [K_{m-1}(a^{1/p}, b_m^{1/p}) : K_{m-1}] \leq p^2.$$

Combine (5) and (6) to conclude that (6) consists of equalities. In particular, a and b_m are p-independent in K_{m-1}. □

LEMMA 2.7.5: *The following conditions on a field K of positive characteristic p are equivalent:*
(a) *The imperfect exponent of K is at most* 1.
(b) *Every finite extension of K has a primitive element.*
(c) *If K is algebraically closed in a field extension F, then F is regular over K.*

Proof: If K is perfect, then (a), (b), and (c) are true. Therefore, we may assume $\text{char}(K) = p > 0$ and K is imperfect.

Proof of "(a) $\Longrightarrow$ (b)": By assumption, $[K^{1/p} : K] = [K : K^p] = p$. Hence, $K_1 = K^{1/p}$ is the unique purely inseparable extension of K of degree p. Moreover, $K_1 = K(a^{1/p})$ for some $a \in K$, so $K_n = K(a^{1/p^n})$ is a purely inseparable extension of K of degree p^n.

Assume that for each $m \leq n$, K_m is the unique purely inseparable extension of K of degree p^m. Let L be a purely inseparable extension of K of degree p^{n+1}. If we prove that $L = K_{n+1}$, then we may conclude by induction that each finite purely inseparable extension of K has a primitive element.

To this end choose $x \in L \setminus K_n$. Let m be the smallest positive integer with $x^{p^m} \in K$. Then $K(x)$ is a purely inseparable extension of K of degree p^m. If $m \leq n$, then by the induction hypothesis $K(x) = K_m \subseteq K_n$, so $x \in K_n$. This contradiction proves that $m = n + 1$ and $L = K(x)$.

The same argument implies that $x^p \in K_n$. Hence, with $q = p^n$, we have $x^p = \sum_{i=0}^{q-1} c_i a^{i/p^n}$ for some $c_0, \ldots, c_{q-1} \in K$. Therefore,

$$x = \sum_{i=0}^{q-1} c_i^{1/p} a^{i/p^{n+1}} \in K_1(a^{1/p^{n+1}}) = K_{n+1}.$$

It follows that $L \subseteq K_{n+1}$. As both fields have degree p^{n+1} over K, they coincide, as desired.

Now let E be a finite extension of K. Denote the maximal separable extension of K in E by E_0. By the primitive element theorem, $E_0 = K(x)$. Since E_0 is both separable and purely inseparable over KE_0^p we have $E_0 = KE_0^p$. Therefore $[E_0 : E_0^p] = [K : K^p] = p$. Apply the first part of the proof

to E_0 and conclude that $E = E_0(y)$, for some element y. Thus, $E = K(x, y)$ with x separable over K. By [Waerden3, §6.10], E/K has a primitive element

Proof of "(b) $\Longrightarrow$ (c)": Let $K(x)$ be a finite extension of K and let $f = \mathrm{irr}(x, K)$. If K is algebraically closed in F, then f remains irreducible over F. Otherwise, its factors would have coefficients algebraic over K and in F, and therefore in K. Thus, F is linearly disjoint from $K(x)$ over K. Hence, (b) implies that F is regular over K.

Proof of "(c) $\Longrightarrow$ (a)": Assume a and b are p-independent elements of K. Then $[K(a^{1/p}, b^{1/p}) : K] = p^2$. Let x and y be transcendental elements over K with $ax^p + by^p = 1$. Put $F = K(x, y)$. By Lemma 2.7.4, K is algebraically closed in F. Hence, by (c), F is regular over K. Therefore, $[F(a^{1/p}, b^{1/p}) : F] = [K(a^{1/p}, b^{1/p}) : K] = p^2$. On the other hand, , $F(a^{1/p}) = F(b^{1/p})$, so $[F(a^{1/p}, b^{1/p}) : F] \leq p$. This contradiction proves that the imperfect exponent of K is at most 1. □

Remark 2.7.6: Relative algebraic closedness does not imply regularity. Let K be a field of positive characteristic p. Suppose K has p-independent elements a, b (e.g. $K = \mathbb{F}_p(t, u)$ where t, u are algebraically independent over $\mathbb{F}_p$). Let x, y be transcendental elements over K with $ax^p + by^p = 1$. Put $F = K(x, y)$. The proof of "(c) $\Longrightarrow$ (a)" then shows that K is algebraically closed in F but F is not linearly disjoint from $K^{1/p}$ over K. Thus, F is not a separable extension of K. A fortiori, F/K is not regular. □

2.8 Derivatives

We develop a criterion for a finitely generated field extension of positive characteristic p to be separable in terms of derivatives..

Definition 2.8.1: A map $D\colon F \to F$ is called a **derivation** of the field F if $D(x + y) = D(x) + D(y)$ and $D(xy) = D(x)y + xD(y)$ for all $x, y \in F$.

If D vanishes on a subfield K of F, then D is a derivation of F **over** K (or a K-**derivation**). □

Let $F(x)$ be a field extension of F and $f \in F[X]$. Suppose D extends to $F(x)$. Then D satisfies the classical chain rule:

$$D(f(x)) = f^D(x) + f'(x)D(x), \tag{1}$$

where f^D is the polynomial obtained by applying D to the coefficients of f and f' is the usual derivative of f. There are three cases:

Case 1: *x is separably algebraic over F.* Then, with $f = \mathrm{irr}(x, F)$, $f'(x) \neq 0$. By (1), $0 = f^D(x) + f'(x)D(x)$. Thus, D extends uniquely to $F(x)$.

Case 2: *x is transcendental.* Then D extends to $F(x)$ by rule (1) and $D(x)$ may be chosen arbitrarily.

CASE 3: *x satisfies $x^{p^m} = a \in F$, for some m.* Then D extends to $F(x)$ if and only if $D(a) = 0$. In this case $D(x)$ may be chosen arbitrarily.

LEMMA 2.8.2: *A necessary and sufficient condition for a finitely generated extension F/K to be separably algebraic is that 0 is the only K-derivation of F.*

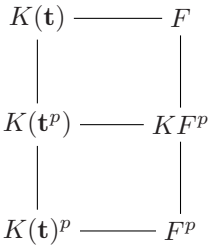
Proof: Necessity follows from Case 1.

Now suppose F/K is not separably algebraic. Then we may write $F = K(x_1, \ldots, x_n)$ such that x_i is transcendental over $K(x_1, \ldots, x_{i-1})$ for $i = 1, \ldots, k$, x_i is separably algebraic over $K(x_1, \ldots, x_{i-1})$ for $i = k+1, \ldots, l$, and x_i is purely inseparable over $K(x_1, \ldots, x_{i-1})$ for $i = l+1, \ldots, n$. Moreover, either $n > l$ or $n = l$ and $k > 0$. If $n > l$, then Case 1 allows us to extend the zero derivation of $K(x_1, \ldots, x_{n-1})$ to a nonzero derivation of F. If $n = l$ and $k > 0$, then by Case 2, the zero derivation of $K(x_1, \ldots, x_{k-1})$ extends to a nonzero derivation D of $K(x_1, \ldots, x_k)$. Applying Case 3 several times, we may then extend D to a derivation of F. □

LEMMA 2.8.3: *Let F/K be a finitely generated extension of positive characteristic p and transcendence degree n. Then F/K is separable if and only if $[F : KF^p] = p^n$. In this case $t_1, \ldots, t_n$ form a p-basis for F over KF^p if and only they form a separating transcendence basis for F/K.*

Proof: Suppose first $[F : KF^p] = p^n$. Let $t_1, \ldots, t_n$ be a p-basis for F/KF^p. Every derivation D of F vanishes on F^p. If D vanishes on $K(\mathbf{t})$, it vanishes on $F = K(\mathbf{t}) \cdot F^p$. By Lemma 2.8.2, $F/K(\mathbf{t})$ is separably algebraic and $t_1, \ldots, t_n$ is a separating transcendence basis for F/K.

Conversely, suppose F/K is separable. Let $t_1, \ldots, t_n$ be a separating transcendence basis for F/K. The extension $F/K(\mathbf{t}) \cdot KF^p$ is both separable and purely inseparable. Hence, $F = K(\mathbf{t}) \cdot KF^p$. Since $F^p/K(\mathbf{t})^p$ is separably algebraic and since $K(\mathbf{t}^p)F^p = KF^p$, we conclude that $KF^p/K(\mathbf{t}^p)$ is separably algebraic.



Therefore, KF^p is linearly disjoint from $K(\mathbf{t})$ over $K(\mathbf{t}^p)$, and $[F : KF^p] = [K(\mathbf{t}) : K(\mathbf{t}^p)] = p^n$. Moreover, $\mathbf{t}$ is a p-basis for F/KF^p. □

COROLLARY 2.8.4: *Let F/K be a finitely generated separable extension of positive characteristic p and let $t \in F$.*

(a) *If there exists a derivation D of F/K such that $D(t) \neq 0$, then F is a separable extension of $K(t)$.*

(b) *If t is transcendental over K and $F/K(t)$ is separable, then there exists a derivation D of F/K such that $D(t) \neq 0$.*

Proof of (a): By assumption, $t \notin KF^p$. Let $n = \text{trans.deg}(F/K)$. By Lemma 2.8.3, $[F : KF^p] = p^n$. Hence, t can be extended to a p-basis $t, t_2, \ldots, t_n$ for F/KF^p. Again, by Lemma 2.8.3, $t, t_2, \ldots, t_n$ is a separating transcendence basis for F/K. Therefore, F is a separable extension of $K(t)$.

Proof of (b): Let $t_2, \ldots, t_n$ be a separating transcendence basis for $F/K(t)$. By Case 2, there exists a derivation D_0 of $K(t, t_2, \ldots, t_n)/K$ such that $D_0(t) = 1$, $D_0(t_2) = 0$, $\ldots$, $D_0(t_n) = 0$. By Case 1, D_0 extends to a derivation D of F/K. $\square$

Exercises

1. Let O be a valuation ring of a field F and consider the subset $\mathfrak{m} = \{x \in O \mid x^{-1} \notin O\}$. Show that if $x \in \mathfrak{m}$ and $a \in O$, then $ax \in \mathfrak{m}$. Prove that $\mathfrak{m}$ is closed under addition. Hint: Use the identity $x + y = (1 + xy^{-1})y$ for $y \neq 0$. Show that $\mathfrak{m}$ is the unique maximal ideal of O.

2. Use Exercise 1 to prove that every valuation ring is integrally closed.

3. Let v be a valuation of $\mathbb{Q}$. Observe that $v(n) \geq v(1) = 0$, for each $n \in \mathbb{N}$. Hence, there exists a smallest $p \in \mathbb{N}$ such that $v(p) > 0$. Prove that p is a prime element of O_v and v is equivalent to v_p. Hint: If a positive integer m is relatively prime to p, then there exist $x, y \in \mathbb{Z}$ such that $xp + ym = 1$.

4. Let v be a valuation of the rational function field $F = K(t)$ which is trivial on K. Suppose there exists $p \in K[t]$ with $v(p) > 0$. Now suppose p has smallest degree with this property. Show that v is equivalent to v_p. Otherwise, there exists $f \in K[t]$ such that $v(f(t)) < 0$. Conclude that $v(t) < 0$, and that v is equivalent to v_∞.

5. Let F/E be a field extension, w a valuation of F, and $x_1, \ldots, x_e$ elements of F such that $w(x_1), \ldots, w(x_e)$ represent distinct classes of $w(F^\times)$ modulo $w(E^\times)$. Show that $x_1, \ldots, x_e$ are linearly independent over E. Thus, $(w(F^\times) : w(E^\times)) \leq [F : E]$. Hint: Use (4b) of Section 2.1.

6. Let Δ be an ordered group containing $\mathbb{Z}$ as a subgroup of index e. Show there exists no positive element $\delta \in \Delta$ such that $e\delta < 1$. Conclude that Δ contains a smallest positive element and hence that $\Delta \cong \mathbb{Z}$. Combine this with Exercise 5 to prove that if the restriction of w to E is discrete, then w is discrete.

7. In the notation of Exercise 5, let v be the restriction of w to E. Let $y_1, \ldots, y_f$ be elements of F with $w(y_1), \ldots, w(y_f) \geq 0$ with residue classes $\bar{y}_1, \ldots, \bar{y}_f$ linearly independent over $\bar{E}_v$. Show that $y_1, \ldots, y_f$ are linearly independent over E. Conclude that $[\bar{F}_w : \bar{E}_v] \leq [F : E]$. Hint: If $a_1, \ldots, a_f \in$

F are not all zero, then there exists j, $1 \le j \le f$ such that $v(\frac{a_1}{a_j}), \dots, v(\frac{a_f}{a_j}) \ge 0$.

8. Let v be a discrete valuation of a field K and let w be an extension of v to a finite Galois extension L of K. Assume that w' is also an extension of v to L such that $w' \ne \sigma(w)$ for all $\sigma \in \mathrm{Gal}(L/K)$. Combine Exercise 7 with Proposition 2.1.1 to produce $x \in L$ such that $w'(x) > 0$ and $w(\sigma x - 1) > 0$ for all $\sigma \in \mathrm{Gal}(L/K)$. With $y = N_{L/K}(x)$, conclude that the former condition gives $v(y) > 0$, while the latter implies $v(y-1) > 0$. Use this contradiction to prove that $\mathrm{Gal}(L/K)$ acts transitively on the extensions of v to L.

9. Let $L, K_1, \dots, K_n$ be extensions of a field K. Let $L_i = K_i L$, $i = 1, \dots, n$. Suppose K_i is linearly disjoint from L over K for $i = 1, \dots, n$ and $L_1, \dots, L_n$ are linearly disjoint over L. Prove that $K_1, \dots, K_n$ are linearly disjoint over K.

10. Let v be a discrete valuation of a field K and let L and M be two finite extensions of K such that v is unramified in L and totally ramified in M. Prove that L and M are linearly disjoint over K. Hint: Consider the Galois hull $\hat{L}$ of L/K.

11. Let E be a regular extension of a perfect field K and let F be a purely inseparable extension of E. Prove that F/K is a regular extension.

12. Let K be a field algebraically closed in an extension F. Prove that $K(x)$ is linearly disjoint from F for every $x \in \tilde{K}$. Hint: Check the irreducibility of $\mathrm{irr}(x, K)$ over F.

13. Prove that a field extension F/K is primary if and only if $FK_{\mathrm{ins}} \cap \tilde{K} = K_{\mathrm{ins}}$. Use this criterion to give another proof to Lemma 2.6.14(a).

14. Let F/K be a finitely generated field extension of characteristic $p > 0$ and of transcendence degree 1. Prove that for each positive integer n, KF^{p^n} is the unique subfield E of F which contains K such that F/E is a purely inseparable extension of degree p^n.

15. (Geyer) The following example shows that Lemma 2.4.8 is false for arbitrary real valuations. Consider the field $\mathbb{Q}_2$ of 2-adic numbers. Show that the field $K = \mathbb{Q}_2(\sqrt[n]{2} \mid n \in \mathbb{N})$ is a totally ramified extension of $\mathbb{Q}_2$ with value group $\mathbb{Q}$. Hence, each extension of K is unramified. Prove that the residue field of both $K(\sqrt{3})$ and $K(\sqrt{-1})$ is $\mathbb{F}_2$. However, their compositum contains $K(\sqrt{-3})$ and therefore has $\mathbb{F}_4$ as its residue field.

Notes

The terminology "algebraic independence" for field extensions replaces "freeness" which we used in [Fried-Jarden3].

Corollary 4 of [Lang4, p. 61] proves Lemma 2.6.15(a) only under the condition (our notation) that E is a separable extension of K.

http://www.springer.com/978-3-540-77269-9

Field Arithmetic
Fried, M.D.; Jarden, M.
2008, XXIV, 792 p., Hardcover
ISBN: 978-3-540-77269-9