Chapter 24

Preliminaries from algebra

24.1 Algebraic field extensions

Take arbitrary field extensions $L|K$ and $F|K$. A homomorphism $L \to F$ will be called a **homomorphism over** K if it fixes K elementwise. An automorphism of L will be called **automorphism of** $L|K$ if it is a homomorphism over K. An element $b \in L$ is **algebraic over** K, if it is the root of some nonzero polynomial f with coefficients from K. For every homomorphism $\sigma : L \to F$ over K, the element σb is again a root of f, hence it is algebraic over K. The **relative algebraic closure of** K **in** L is the subfield of L consisting of all elements which are algebraic over K; in particular, it contains K. We see that every automorphism of $L|K$ sends the relative algebraic closure into itself.

A field extension $L|K$ is called **algebraic** if every element $b \in L$ is algebraic over K. Every **finite field extension** $L|K$ (i.e., $[L : K] < \infty$) is algebraic. A field extension of the form $K(b)|K$ is called **simple**. It is algebraic if and only if b is algebraic over K, and this is the case if and only if the field $K(b)$ is equal to the ring $K[b]$. If $L|K$ and $L'|L$ are algebraic field extensions, then so is $L'|K$. There exist maximal algebraic extensions, called **algebraic closures of** K. An algebraic closure L of K is itself **algebraically closed**, that is, every algebraic extension $L'|L$ is **trivial**: $L' = L$. Over an algebraically closed field, every polynomial splits into linear factors. All algebraic closures of a field K are isomorphic over K, so we shall speak of *the* algebraic closure of K and denote it by $\tilde{K}$. In this sense, the algebraic closure of K coincides with the relative algebraic closure of K in every algebraically closed extension field. We often use such an identification of isomorphic objects without further mentioning. If $\sigma : L \to F$ is a homomorphism over K, then it is injective, and we will call it an **embedding of** L **in** F **over** K. If in addition F is algebraically closed, then σ can be extended to an embedding of $\tilde{L}$ in F over K. In particular, if $L|K$ is algebraic, then every embedding of L in $\tilde{L} = \tilde{K}$ over K can be extended to an automorphism of $\tilde{K}|K$.

Let b be algebraic over K. Then $\{f \in K[X] \mid f(b) = 0\}$ is a non-trivial proper ideal of the ring $K[X]$. Since $K[X]$ is a euclidean ring with respect to the usual degree function for polynomials, this ideal is principal. It has precisely one monic generator f, which is called the **minimal polynomial of** b **over** K**.** (Recall that a polynomial $f = c_n X^n + \ldots + c_1 X + c_0$ is called **monic** if its **leading coefficient** c_n is equal to 1.) Thus, a polynomial $g \in K[X]$ admits b as a zero if and only if f divides g in the ring $K[X]$. In particular, f is irreducible over K. Every embedding σ of $K(b)$ in $\tilde{K}$ over K sends b to a root σb of f. Conversely, if a is a second root of f, then there is an isomorphism σ of the

fields $K(b) = K[b]$ and $K(a) = K[a]$ over K which sends b to a. This isomorphism extends to an automorphism of $\tilde{K}|K$. Hence, the finite set of roots of f in $\tilde{K}$ coincides with the set $\{\sigma b \mid \sigma \text{ is an automorphism of } \tilde{K}|K\}$; its elements are called the **conjugates of** b. Two elements $a, b \in \tilde{K}$ are called **conjugate over** K if there exists an automorphism σ of $\tilde{K}|K$ such that $a = \sigma b$.

Lemma 24.1 *a) Let $g, h \in K[X]$. Then g is prime to h in the ring $K[X]$ if and only if g and h admit no common root in $\tilde{K}$.*

b) Assume that $gh \in K[X]$ with $g, h \in \tilde{K}[X]$ such that g is monic, g and h admit no common root in $\tilde{K}$ and the set of roots of g in $\tilde{K}$ is closed under conjugates. Then $g, h \in K[X]$.

Proof: a): If f is a nonconstant common divisor of g and h, then it admits a root in $\tilde{K}$, which is thus a common root of g and h. Conversely, if b is a common root of g and h in $\tilde{K}$, then the minimal polynomial of b over K divides both g and h, showing that g is not prime to h in $K[X]$.

b): Suppose that we have verified our assertion for all products gh with $\deg g < n$ (for $\deg g = 1$, the assertion is trivial). Now let g be of degree n and gh satisfy the assumptions of part b). Let b be a root of g in $\tilde{K}$. Since it is also a root of $gh \in K[X]$, the minimal polynomial f of b over K must divide gh. Every root of f is a conjugate of b over K and by assumption, it is also a root of g. If it appears m times in f, then it also appears m times in g, because g and h have no roots in common. Hence, f divides g in $\tilde{K}[X]$. So we can write $gh = f\tilde{g}h$ with $\tilde{g} \in \tilde{K}[X]$ of degree $< n$. Since f and gh are elements of $K[X]$, we can apply the euclidean algorithm (or in other words, the polynomial division with remainder) to f and gh in $K[X]$. The result can not be different from the result in the ring $\tilde{K}[X]$, which shows that $\tilde{g}h \in K[X]$. Now we can apply the induction hypothesis to conclude that $\tilde{g}, h \in K[X]$ and thus also $g = f\tilde{g} \in K[X]$. □

If $\mathcal{P}$ is any property of field extensions, then we will say that $L|K$ is a **tower of extensions with property** $\mathcal{P}$ if there are intermediate fields $K = K_0 \subset K_1 \subset \ldots \subset K_n = L$ such that $K_i|K_{i-1}$ are extensions with property $\mathcal{P}$, for $i = 1, \ldots, n$.

In the following, let $L|K$ be an algebraic extension, not necessarily finite. It is called **normal** if every automorphism of $\tilde{K}|K$ sends L into itself. In particular, $\tilde{K}|K$ is normal. If $K'|K$ is a subextension of $L|K$ and $L|K$ is normal, then also $L|K'$ is normal since every automorphism of $\tilde{K}|K'$ is an automorphism of $\tilde{K}|K$. On every simple extension $K(b)$ of K, the restriction of a given automorphism σ of $\tilde{K}|K$ is uniquely determined by the root σb of the minimal polynomial of b over K. Consequently, $K(b)|K$ is normal if and only if all conjugates of b lie in $K(b)$. Moreover, it shows that the embeddings of $K(b)$ in $\tilde{K}$ over K correspond bijectively to the roots of the minimal polynomial f of b over K. Since $\deg f$ is equal to the degree $[K(b) : K]$ of the extension $K(b)|K$, and since f has at most $\deg f$ many distinct roots in $\tilde{K}$, it follows that there are at most $[K(b) : K]$ distinct embeddings of $K(b)$ in $\tilde{K}$ over K.

As $L|K$ is algebraic, every element $b \in L$ is already contained in the finite algebraic subextension $K(b)|K$. This shows that L is the union over all finite subextensions. So we can write $L = \bigcup_{i \in I} L_i$ where L_i runs through all finite extensions of K which are contained in L (the index set may be taken e.g. to be a subset of the cardinal $2^{|L|}$). But it also suffices to take the fields L_i to be simple extensions of K. On the other hand, every finite extension

$L|K$ is a tower of simple extensions. The degree of field extensions is multiplicative, that is, if $L|K'$ and $K'|K$ are finite extensions, then $[L : K] = [L : K'] \cdot [K' : K]$. Since also the number of embeddings is multiplicative in a similar way, one deduces by induction on the extensions in the tower that every finite extension $L|K$ admits at most $[L : K]$ distinct embeddings in $\tilde{K}$ over K. The number of distinct embeddings is called the **separable degree of** $L|K$, denoted by $[L : K]_{\text{sep}}$. If $[L : K] = [L : K]_{\text{sep}}$, then $L|K$ is called **separable**. Hence $K(b)|K$ is separable if and only if the minimal polynomial of b has no multiple roots; in this case, the element b and its minimal polynomial are called **separable over** K. At the other extreme, an arbitrary algebraic extension $L|K$ is called **purely inseparable** if it only admits one embedding in $\tilde{K}$ over K (which is the identity if we assume L to lie in $\tilde{K}$, as we usually do). Hence $K(b)|K$ is purely inseparable if and only if its separable degree is 1, i.e. if the minimal polynomial of b admits only b as a root; in this case, the element b and its minimal polynomial are called **purely inseparable over** K. We note that

The extension $L|K$ is purely inseparable if and only if every $b \in L$ is purely inseparable over K.

Indeed, if $K(b)$ would admit two distinct embeddings in $\tilde{K}$ over K, then these could be extended to distinct embeddings of L in $\tilde{K}$ over K. If on the other hand, $L|K$ admits two distinct embeddings, then there must be some $b \in L$ on which these act differently.

An element a is a multiple root of a polynomial f if and only if it is also a root of the derivative f' of f. If a is a simple root of some polynomial over K, then it is also a simple root of its minimal polynomial over K. Hence, an element a in an arbitrary extension of K is separable algebraic over K if (and only if) there is some $f \in K[X]$ such that $f(a) = 0$ and $f'(a) \neq 0$. See Lemma 9.12 for a "multidimensional" version of this criterion, working simultaneously for n elements by use of n polynomials.

If $L|K$ is finite and separable, then it is simple (cf. [LANG3], Chapter VII, §6, Theorem 14). An element $b \in L$ satisfying $L = K(b)$ is called a **primitive element**.

Like the degree $[L : K]$, also the separable degree $[L : K]_{\text{sep}}$ is multiplicative, that is, if $L|K'$ and $K'|K$ are finite extensions, then $[L : K]_{\text{sep}} = [L : K']_{\text{sep}} \cdot [K' : K]_{\text{sep}}$. From this, it follows that $L|K$ is separable if and only if $L|K'$ and $K'|K$ are separable. In particular, every subextension of a finite separable extension is separable. So we may generalize our definition as follows: An arbitrary algebraic extension $L|K$ is called **separable** if every finite subextension $L_i|K$ is separable. If $L|K$ is separable and normal, then we will call it a **Galois extension**. Since we are concerned with infinite Galois theory, we do not require the property "finite" for Galois extensions. If $L|K$ is normal, then we shall use the notation $\operatorname{Gal} L|K$ for the group of all automorphisms of $L|K$, and we call it the **Galois group of** $L|K$, even if $L|K$ is not separable. We use the abbreviation $\operatorname{Gal} K$ for $\operatorname{Gal} \tilde{K}|K$ and call it the **absolute Galois group of** K.

Later, we will define the notion "separable" also for arbitrary, not necessarily algebraic extensions. So we will speak henceforth of **separable algebraic** extensions if we want to restrict our arguments to algebraic extensions. In contrast to this, **purely inseparable** and **normal** will always mean that the extension is algebraic.

Let 1 denote the multiplicative unit in the field K and $n \cdot 1$ the result of adding it up n times. If there is a smallest number p such that $p \cdot 1 = 0$, then p is a prime number; it is called the **characteristic** of K. If there is no such p, then we say that the characteristic of K is 0. If the characteristic of K is $p > 0$, then the smallest field contained in K is $\mathbb{F}_p$,

the field with p elements. If the characteristic of K is 0, then the smallest subfield of K is $\mathbb{Q}$, the rationals. The smallest subfield of K is called the **prime field of** K. A field extension $L|K$ is called **finitely generated** if $L = K(x_1, \ldots, x_n)$ for suitable elements $x_1, \ldots, x_n \in L$. Every finitely generated algebraic extension is a finite extension. The field K is called a **finitely generated field** if it is a finitely generated field extension of its prime field.

Assume $L|K$ to be a Galois extension of degree p a prime which is not equal to the characteristic of K. If K contains a primitive p-th root of unity, then L contains an element b such that $c := b^p \in K$ and $L = K(b)$. The minimal polynomial of b over K is $X^p - c$. This follows from **Kummer Theory**; cf. [LANG3], Chapter VIII, §8. Now assume that $L|K$ is a Galois extension of degree $p = \operatorname{char} K$. Then L contains an element b such that $c := b^p - b \in K$ and $L = K(b)$. This assertion is a special case of a more general result proved in Section 12.6; see Corollary 12.29. See also [LANG3], Chapter VIII, §8. The minimal polynomial of b over K is $X^p - X - c$. Such a polynomial is called an **Artin-Schreier polynomial**. The extension is said to be an **Artin-Schreier extension**, and b is an **Artin-Schreier root of** f and an **Artin-Schreier generator of** $L|K$. We frequently use the abbreviation $\wp(X)$ for the polynomial $X^p - X$. This polynomial is **additive**, that is, $\wp(b + b') = \wp(b) + \wp(b')$ for all $b, b' \in L$. This is a consequence of the additivity of the **Frobenius endomorphism** $x \mapsto x^p$ of a field of characteristic p; see Section 24.7 below. Note in particular that if b is a root of $X^p - X - c$ and b' is a root of $X^p - X - c'$, then $b + b'$ is a root of $X^p - X - (c + c')$. From the special case $c' = 0$ we see that the roots of $X^p - X - c$ are of the form $b + b'$ with b' a root of $X^p - X$. We can observe at once that 0 and 1 are roots of $X^p - X$. But in view of the additivity, if 1 is a root, then also $n \cdot 1$ for every $n \in \mathbb{N}$. Since the characteristic of K was assumed to be p, the roots of $X^p - X$ are precisely $0, 1, \ldots, p - 1$. Consequently:

Lemma 24.2 *Let K be a field of characteristic $p > 0$ and $b \in \tilde{K}$ a root of the Artin-Schreier polynomial $X^p - X - c$ with $c \in K$. Then all roots of $X^p - X - c$ are given by $b, b + 1, \ldots, b + p - 1$. In particular, if $X^p - X - c$ has a root in K, then it splits over K into linear factors.*

We also use the name "Artin-Schreier extension" for certain extensions of valued fields of characteristic 0; see Section 6.5 for the definition.

Take two subextensions $E|K$ and $F|K$ of an arbitrary field extension $\Omega|K$. The intersection $E \cap F$ is again a subfield of Ω containing K. The **field compositum of** E **and** F **(in** Ω**)**, denoted by $E.F$, is the smallest subfield of Ω which contains both E and F. If $E.F = \Omega$ and $E \cap F = K$, then E is called a **field complement for** F **in** Ω **over** K**.** Note that every two arbitrary field extensions of K can be embedded in a common extension field Ω (that is, the theory of fields has the amalgamation property, see Section 24.5). In this extension field, their field compositum can be defined as above. But it may depend on the embeddings (for instance, distinct embeddings of non-normal algebraic extensions may produce non-isomorphic composita). Every element in the field compositum can be written as $(x_1y_1 + \ldots + x_my_m)/(x'_1y'_1 + \ldots + x'_ny'_n)$ for suitable $m, n \in \mathbb{N}$ and $x_i, x'_i \in E$, $y_i, y'_i \in F$. If both extensions $E|K$ and $F|K$ are algebraic, then so is $E.F|K$. If they are normal in addition, then every automorphism of $\tilde{K}|K$ sends E and F and hence also $E.F$ into itself, showing that also $E.F|K$ is normal.

Let $L|K$ be an algebraic and $K'|K$ an arbitrary field extension. Then $\widetilde{K'}$ contains $\tilde{K} = \tilde{L}$ and thus, we can take the compositum $L.K'$ inside $\widetilde{K'}$ (again, it depends on the

embedding of L in $\tilde{K}$, and there are different composita if $L|K$ is not normal). Every basis of $L|K$ is also a system of generators of $L.K'|K'$, but it may not be a basis anymore. So if $L|K$ is finite, we have that

$$[L.K' : K'] \leq [L : K] .$$

In other words, the minimal polynomial of an element $b \in L$ may not be irreducible over K', but as we know already, it is divided by the minimal polynomial of b over K'. If $[L.K' : K'] = [L : K]$, then it follows that for every element $b \in L$ its minimal polynomial over K will be irreducible over K' and thus be the minimal polynomial of b over K'. Otherwise, we would have that $[K'(b) : K'] < [K(b) : K]$ which yields that $[L.K' : K'] = [L.K' : K'(b)] \cdot [K'(b) : K'] < [L.K' : K'(b)] \cdot [K(b) : K] \leq [L : K(b)] \cdot [K(b) : K] = [L : K]$ since $K'(b) = K(b).K'$. It follows that if $[L.K' : K'] = [L : K]$ and $L.K'|K'$ is separable resp. purely inseparable, then so is $L|K$.

Even in the case of an infinite algebraic extension $L|K$, every finite subextension $L'|K'$ of $L.K'|K'$ is contained in $L_i.K'|K'$ for some finite subextension $L_i|K$ of $L|K$. Indeed, L' is generated over K' by finitely many elements $b_1, \ldots, b_n \in L.K'$. To write down the elements $b_1, \ldots, b_n$, only finitely many elements $c_1, \ldots, c_k \in L$ (and finitely many elements in K') are needed. Hence, $L_i := L(c_1, \ldots, c_k)$ is a finite extension of L, and $L' \subset L_i.K'$. Now assume in addition that $L|K$ is separable. Then also $L_i|K$ is separable, and it is thus simple; let b be a primitive element. Then the minimal polynomial f of b over K has no multiple root. The same is true for the minimal polynomial of b over K' since it is a divisor of f. This shows that $K'(b)|K'$ and thus also its subextension $L'|K'$ is separable. In this way, it is shown that every finite subextension of $L.K'|K'$ is separable algebraic. We have thereby proved:

If $L|K$ is separable algebraic and $K'|K$ is an arbitrary field extension, then $L.K'|K'$ is separable algebraic.

It follows by induction that the compositum of finitely many separable algebraic extensions is again separable. In particular, if every extension $K(b)|K$ for $b \in L$ is separable, then so is every finite subextension $L|K$ since it is the compositum of finitely many simple subextensions. Conversely, if $L|K$ is separable, then so is the finite subextension $K(b)|K$. We have proved:

The extension $L|K$ is separable if and only if every $b \in L$ is separable over K.

We shall now prove the **transitivity of separable extensions**:

Lemma 24.3 *Let $L|K$ be an algebraic extension with subextension $K'|K$. Then $L|K$ is separable if and only if $L|K'$ and $K'|K$ are separable.*

The proof of this lemma uses a typical argument which connects finite with infinite extensions. For later use, we formulate this argument in more generality than we need it here.

Lemma 24.4 *Let $K'|K$ be an arbitrary and $L'|K'$ a finite extension. Then there exists a finitely generated subextension $K_0|K$ of $K'|K$ and a finite subextension $L_0|K_0$ of $L'|K_0$ such that $L' = L_0.K'$ and $[L' : K'] = [L_0 : K_0]$. It follows that if $L'|K'$ is separable resp. purely inseparable, then so is $L_0|K_0$.*

If $S_{K'}$ and $S_{L'}$ are any finite sets of elements in K' and L' respectively, then K_0 and L_0 can be chosen such that $S_{K'} \subset K_0$ and $S_{L'} \subset L_0$. If $K'|K$ is algebraic, then $K_0|K$ and $L_0|K$ are finite.

Proof: Without loss of generality, we can enlarge the set $S_{L'}$ by finitely many elements such that it generates the finite extension $L'|K'$. Write $S_{L'} = \{b_1, \ldots, b_n\}$. Now we form a finite set S_1 of elements in K' by adjoining to $S_{K'}$ the coefficients of the minimal polynomial of b_1 over K'. Every element of $K'(b_1, \ldots, b_k)$ is a rational function in $b_1, \ldots, b_k$ which involves finitely many coefficients from K'. So for $1 \leq k < n$, we form S_{k+1} by adjoining to S_k the finitely many elements of K' that appear as coefficients in the rational functions which are the coefficients of the minimal polynomial of b_{k+1} over $K'(b_1, \ldots, b_k)$. We obtain a finite set S_n of elements in K', and we set $K_0 := K(S_n)$. We obtain that $[K'(b_1) : K'] = [K_0(b_1) : K_0]$ and $[K'(b_1, \ldots, b_{k+1}) : K'(b_1, \ldots, b_k)] = [K_0(b_1, \ldots, b_{k+1}) : K_0(b_1, \ldots, b_k)]$ for $1 \leq k < n$. It follows that $L_0 := K_0(b_1, \ldots, b_n) = K_0(S_{L'})$ satisfies $L' = L_0.K'$ and $[L' : K'] = [L_0 : K_0]$. By construction, $S_{K'} \subset K_0$ and $S_{L'} \subset L_0$. Further, $K_0|K$ is a finitely generated subextension of $K'|K$. If the latter is algebraic, then also $K_0|K$ is algebraic and thus finite.

The assertion about separability resp. inseparability follows directly from the equality $[L' : K'] = [L_0 : K_0]$, as we have shown earlier. □

Now we are able to prove Lemma 24.3. Let $L|K$ be algebraic with subextension $K'|K$. Assume first that $L|K$ is separable. Then it follows directly from the definition that also $K'|K$ is separable. Let $L'|K'$ be a finite subextension of $L|K'$, and choose K_0 and L_0 as in the above lemma. Then $L_0|K$ is a finite extension, so it is separable since $L|K$ is supposed to be separable. By what we have shown earlier, $L' = L_0.K'$ is separable over K'. This proves that $L|K'$ is separable.

For the converse, assume that $L|K'$ and $K'|K$ are separable. Let $E|K$ be a finite subextension of $L|K$ and $L' = E.K'$. As a finite subextension of $L|K'$, the extension $L'|K'$ is separable and thus simple. Let b be a primitive element of $L'|K'$. Then its minimal polynomial over K' has no multiple roots. Choose K_0 and L_0 as in the above lemma such that L_0 contains b and some set of generators of the finite extension $E|K$. Then $E \subset L_0$. Since $K'|K$ is separable, so is its finite subextension $K_0|K$. Since $[L_0 : K_0] = [L' : K'] = [K'(b) : K']$, we see that b also generates L_0 over K_0 and that its minimal polynomial over K_0 is the same as over K'. Since this minimal polynomial has no multiple roots, it follows that $L_0|K_0$ is separable. By what we have proved already about finite extensions, $L_0|K$ and thus also $E|K$ is separable. This completes our proof. □

If $E|K$ is an arbitrary subextension of a Galois extension $L|K$, then $L|E$ is separable and normal and thus again a Galois extension (since $L.E = L$). In this case, $\operatorname{Gal} L|E$ may be identified in a natural way with the subgroup $\{\sigma \in \operatorname{Gal} L|K \mid \forall x \in E : \sigma x = x\}$ of $\operatorname{Gal} L|K$. For $\sigma \in \operatorname{Gal} L|K$, the **restriction** of σ to E will be denoted by $res_E(\sigma)$. If $E|K$ is normal, then the restriction map

$$\operatorname{res}_E : \operatorname{Gal} L|K \longrightarrow \operatorname{Gal} E|K$$

is a group epimorphism since every automorphism of $E|K$ can be extended to an automorphism of $L|K$. Note that $\operatorname{Gal} L|E = \operatorname{res}_E^{-1}(1)$.

If $E|K$ and $F|K$ are separable algebraic extensions, then by what we have shown, $E.F|F$ is separable and thus, $E.F|K$ is separable. That is, *the compositum of two separable algebraic extensions is again separable algebraic.* Since we have shown the analogue also for normal extensions, we conclude that *the compositum of two Galois extensions is again a*

Galois extension. It also follows that an algebraic extension $L|K$ generated by the elements b_i, $i \in I$, is normal (resp. separable) if and only if every extension $K(b_i)|K$ is. Further, we see that the composition of all separable algebraic subextensions of an arbitrary extension $L|K$ is itself a separable algebraic subextension of $L|K$, and it is thus the maximal one. We will call it the **relative separable-algebraic closure of K in L** and denote it by $(L|K)^{\rm sep}$. In fact, $(L|K)^{\rm sep}$ consists of all elements $b \in L$ such that $K(b)|K$ is separable algebraic. The maximal separable algebraic extension of K is $(\tilde{K}|K)^{\rm sep}$; it will be called the **separable-algebraic closure of** K and denoted by $K^{\rm sep}$. It consists of all elements (in $\tilde{K}$) which are separable algebraic over K.

To every algebraic extension $L|K$ we can find a normal extension $L'|K$ containing L. The minimal one is found by adjoining, for every $b \in L$, all roots of the minimal polynomial of b over K. This field L' is called the **normal hull** of L over K. If $L|K$ is finite, then so is $L'|K$. An arbitrary algebraic extension $L|K$ is normal if and only if it contains the normal hull of every finite subextension $L_i|K$. If $L|K$ is normal, then L is the union over all finite normal subextensions; in Section 24.4, we shall describe the connection between their Galois groups and the Galois group of $L|K$.

For every algebraic extension $L|K$, every homomorphism σ of L into L over K is an automorphism of $L|K$. Indeed, it is injective since it is a non-trivial field homomorphism. If $b \in L$ then $\sigma^n b \in L$ for every $n \in \mathbb{N}$. Since b has only finitely many conjugates (and σ is invertible), there is some $n > 0$ such that $\sigma^n b = b$. Hence, $b = \sigma(\sigma^{n-1}b) \in \sigma L$, which proves that σ is surjective.

The following is a criterion for the existence of embeddings of infinite algebraic extensions:

Theorem 24.5 (Compactness Principle for Algebraic Extensions)
Let $L|K$ be an algebraic field extension and $L = \bigcup_{i\in I} L_i$ where the L_i run through all finite subextensions of $L|K$. Let $F|K$ be an arbitrary field extension. If for every $i \in I$, the field L_i admits an embedding ι_i in F over K, then there exists an embedding ι of L in F over K such that

$$\forall i \in I:\ \mathrm{res}_{L_i}(\iota) = \mathrm{res}_{L_i}(\iota_j) \text{ for some } j \in I \text{ such that } L_j \supset L_i\ . \tag{24.1}$$

If $L|K$ is normal then the assertion remains true if we let L_i run through all finite normal subextensions of $L|K$.

We will prove the theorem in the next section using a compactness principle for inverse limits. The following corollary illustrates the use of assertion (24.1). In fact, this assertion implies that the embedding ι inherits the universal properties that all ι_i have in common.

Corollary 24.6 *Let $(L,v)|(K,v)$ be an algebraic and $(F,w)|(K,v)$ an arbitrary extension of valued fields. If every finite subextension of $L|K$ admits a valuation preserving embedding ι in (F,w) over (K,v), then so does (L,v). If in addition, vL admits an embedding ρ in wF over vK and $\overline{L}$ admits an embedding σ in $\overline{F}$ over $\overline{K}$ and if the given embeddings of the finite subextensions respect the corresponding restrictions of ρ and σ, then ι may be chosen as to respect ρ and σ.*

Proof: Since every $b \in L$ is contained in some L_i, the embbeding ι chosen according to the foregoing theorem will satisfy $w\iota b \geq 0 \Leftrightarrow w\iota_j b \geq 0 \Leftrightarrow vb \geq 0$, resp. $(\iota b)w = (\iota_j b)w = \sigma bv$ if $vb = 0$, resp. $w\iota b = w\iota_j b = \rho vb$. □

Exercise 24.1 *Give an example where $L|K'$ and $K'|K$ are finite normal extensions, but $L|K$ is not normal.*

24.2 Inverse limits

Suppose that $(I, \leq)$ is a partially ordered set. A family $\{\mathcal{X}_i, \pi_{ji} \mid i, j \in I\,,\ i \leq j\}$ consisting of topological spaces $\mathcal{X}_i$ and continuous maps $\pi_{ji} : \mathcal{X}_j \to \mathcal{X}_i$ is called an **inverse system** (or **projective system**) if it satisfies

(INV0) for all $i, j \in I$ there is $k \in I$ such that $i \leq k$ and $j \leq k$,

(INV1) π_{ii} is the identity map on $\mathcal{X}_i$ for every $i \in I$,

(INV2) $\pi_{ki} = \pi_{ji} \circ \pi_{kj}$ for all $i, j, k \in I$ such that $i \leq j \leq k$.

The **inverse limit** (or **projective limit**) of an inverse system $\{\mathcal{X}_i, \pi_{ji}\}$ is defined to be the subspace

$$\varprojlim \mathcal{X}_i := \{(x_\ell)_{\ell \in I} \in \prod_{i \in I} \mathcal{X}_i \mid \pi_{ji}(x_j) = x_i \text{ whenever } i \leq j\}$$

of the cartesian product $\prod_{i \in I} \mathcal{X}_i$ which is endowed with the product topology. Recall that the **product topology** is the coarsest topology such that for all $i \in I$, the projection pr_i onto the i-th component $\mathcal{X}_i$ is continuous. It has a basis consisting of all sets of the form $\prod_{i \in I} \mathcal{U}_i$ where $\mathcal{U}_i$ is an open subset of $\mathcal{X}_i$ for all $i \in I$ and $\mathcal{U}_i = \mathcal{X}_i$ for almost all i. If all $\mathcal{X}_i$ are hausdorff, then also the product topology is hausdorff, and $\mathcal{X} := \varprojlim \mathcal{X}_i$ is a closed subspace of the product. The latter is seen as follows. Let $(x_i)_{i \in I} \notin \mathcal{X}$. Then there are $i, j \in I$, $i \leq j$, such that $\pi_{ji}(x_j) \neq x_i$. If $\mathcal{X}_i$ is hausdorff, then we may choose disjoint open neighborhoods $\mathcal{U}_i$ and $\mathcal{U}_i'$ of x_i and $\pi_{ji}(x_j)$ respectively. Now $\mathcal{U}_i \times \pi_{ji}^{-1}(\mathcal{U}_i') \times \prod_{k \neq i,j} \mathcal{X}_k$ is an open neighborhood of $(x_i)_{i \in I}$ whose intersection with $\mathcal{X}$ is empty. This proves that the complement of $\mathcal{X}$ in the product is open. The argument also shows that for $i \leq j$ and $\mathcal{X}_i$ hausdorff, the set $\mathcal{X}_{ji} := \{(x_\ell)_{\ell \in I} \mid \pi_{ji}(x_j) = x_i\}$ is closed in $\prod \mathcal{X}_i$. Observe that

$$\mathcal{X} = \bigcap_{i \leq j} \mathcal{X}_{ji}\ .$$

Lemma 24.7 *The inverse limit $\mathcal{X}$ of an inverse system of nonempty compact hausdorff spaces $\mathcal{X}_i$ is a nonempty compact hausdorff space.*

Proof: By Tychonoff's Theorem, the product of the compact spaces $\mathcal{X}_i$ is compact. Since all $\mathcal{X}_i$ are assumed to be hausdorff, their product is also hausdorff, and $\mathcal{X}$ is a closed subspace of the product, as we have seen above. Hence, $\mathcal{X}$ is hausdorff and compact. It remains to show that $\mathcal{X}$ is nonempty. By the compactness of the product space, this will follow if we are able to show that the intersection of finitely many of the closed sets $\mathcal{X}_{ji}$ is nonempty. In such a finite intersection, only finitely many indeces $i, j \in I$ are involved, and by (INV0) we may choose $k \in I$ which is bigger than all of them. Since $\mathcal{X}_k$ is nonempty by assumption, the set $\{(x_i)_{i \in I} \mid x_k \in \mathcal{X}_k \text{ and } \pi_{ki}(x_k) = x_i \text{ whenever } i \leq k\}$ is a nonempty subset of the intersection. □

The restriction of the projection pr_i to $\mathcal{X}$ is a map from $\mathcal{X}$ into $\mathcal{X}_i$ and will be denoted by π_i. These maps satisfy $\pi_i = \pi_{ji} \circ \pi_j$ whenever $i \leq j$. Observe that axiom (INV0) plays a crucial role in the above proof. Using again this axiom, the reader may show that a basis for the topology of $\mathcal{X}$ is given by the sets $\pi_i^{-1}(\mathcal{U}_i)$ where $i \in I$ and $\mathcal{U}_i$ is an open subset of $\mathcal{X}_i$. (For the product space, the sets $\mathrm{pr}_i^{-1}(\mathcal{U}_i)$ will in general only form a subbasis.)

Note that the foregoing lemma immediately applies to the case of finite sets $\mathcal{X}_i$ because they are compact under the discrete topology. This is the case of most of our applications. In particular, we are now able to prove the Compactness Principle for Algebraic Extensions.

Proof of Theorem 24.5: Let the notations be as in that theorem. We order I by defining $i \leq j :\Leftrightarrow L_i \subset L_j$. Then (INV0) is satisfied since every two finite extensions L_i, L_j are contained in the finite extension $L_i . L_j$ which is equal to L_k for some $k \in I$. (The same argument works for the finite normal extensions.) For $i \in I$, we take $\mathcal{X}_i$ to consist of all embeddings of L_i in F over K which are the restriction of ι_j to L_i for some $j \geq i$. The map π_{ji} is just given by restricting an embedding of L_j to the subfield L_i. Then axioms (INV1) and (INV2) are satisfied. Since every $L_i|K$ is a finite extension, every $\mathcal{X}_i$ is finite; it is nonempty since it contains ι_i. An application of Lemma 24.7 now shows that the inverse limit of $\{\mathcal{X}_i\,,\,\pi_{ji}\}$ is nonempty. Let $(\tau_i)_{i\in I}$ be an element of it. We define an embedding of L in F over K as follows. For every $a \in L$ we find some $i \in I$ such that $a \in L_i$, and we set $\iota a = \tau_i a$. The fact that $(\tau_i)_{i\in I}$ is an element of the inverse limit, guarantees that ι is welldefined. We have $\mathrm{res}_{L_i}(\iota) = \tau_i$ which by definition of $\mathcal{X}_i$ is the restriction of ι_j for some $j \geq i$. □

Note that the proof also indicates the existence of a bijection between the set of all embeddings of L in F over K and the inverse limit of $\{\mathcal{X}_i\,,\,\pi_{ji}\}$ where $\mathcal{X}_i$ is the set of all embeddings of L_i in F over K. The above proof shows how to associate an embedding to every element of the inverse limit. Surjectivity follows from the fact that for ι an embedding of L, the restrictions $\pi_i\iota$ of ι to L_i are compatible with the restrictions π_{ji}, that is, $\pi_{ji}\pi_j\iota = \pi_i\iota$. Injectivity follows from the fact that every element of L is contained in some L_i.

Setting $F = L$ and assuming that $L|K$ is normal, we obtain a bijection between $\mathrm{Gal}\, L|K$ and the inverse limit of $\{\mathrm{Gal}\, L_i|K\,,\,\pi_{ji}\}$ where the L_i run through all finite normal subextensions of $L|K$ and the maps $\pi_{ji} : \mathrm{Gal}\, L_j|K \to \mathrm{Gal}\, L_i|K$ are again given by restriction. Note that in this case they are surjective since every automorphism of $L_i|K$ may be extended to an automorphism of $L_j|K$ if $L_i \subset L_j$. The inverse limit inherits the group structure of the groups $\mathrm{Gal}\, L_i|K$ by componentwise composition (since composition commutes with restriction). With this group structure, the above bijection turns into a group isomorphism

$$\mathrm{Gal}\, L|K \cong \varprojlim \mathrm{Gal}\, L_i|K\ .$$

For every i, the map π_i is the restriction $\mathrm{res}_{L_i} :\ \mathrm{Gal}\, L|K \to \mathrm{Gal}\, L_i|K$.

24.3 Topological and profinite groups

A **topological group** is a group G endowed with a topology such that the maps $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ are continuous. It follows that for every $g \in G$, the maps $x \mapsto gx$, $x \mapsto xg$ and $x \mapsto x^{-1}$ are homeomorphisms. Hence, a subgroup H of G is open if and only if the coset gH is open, and the same holds for "closed" in the place of "open". A closed

subgroup H of finite index in G is open since its complement is the union of finitely many cosets $gH \neq H$ and every coset gH is a closed set. Conversely, every open subgroup H is closed since its complement is the union of the open cosets $gH \neq H$. In every compact topological group an open subgroup H must be of finite index. Indeed, the cosets gH form an open covering of G, and since it does not admit a proper subcovering, it must itself be finite, that is, there are only finitely many cosets. Hence for compact topological groups, the open subgroups are precisely the closed subgroups of finite index.

By a **topological isomorphism** of topological groups we will mean a **continuous** group isomorphism with continuous inverse. In particular, a topological isomorphism is a homeomorphism. Note that a group homomorphism $f : G \to G_1$ of topological groups is continuous if and only if for every (open) neighborhood U_1 of $1 \in G_1$ there exists a neighborhood U of $1 \in G$ such that $f(U) \subset U_1$. Similarly, f is **open** if and only if for every (open) neighborhood U of $1 \in G$ there exists a neighborhood U_1 of $1 \in G_1$ such that $U_1 \subset f(U)$. This follows from the fact that for every element $g \in G$, the neighborhood filter of 1 is sent onto the neighborhood filter of g by the homeomorphism $x \mapsto gx$.

Let us require in addition for a topological group G that the subset $\{1\}$ be closed. Then for every $g \in G$, the subset $\{g\}$ is closed. With this proviso, topological groups have the following properties.

Every topological group is hausdorff. Indeed, let $a, b \in G$ with $a \neq b$. Then $G \setminus \{b\}$ is an open neighborhood of a. By the continuity of $(x, y) \mapsto xy$ there exist open neighborhoods U_a of a and U_1 of 1 such that $U_a \cdot U_1 \subset G \setminus \{b\}$. It follows that $U_a \cap bU_1^{-1} = \emptyset$. Since $x \mapsto x^{-1}$ is a homeomorphism, bU_1^{-1} is an open neighborhood of b.

The kernel of a continuous homomorphism of topological groups is a closed normal subgroup since it is the preimage of the closed set $\{1\}$. For the facts stated in the following, cf. [PON], Chapter III, §20. If H is a closed normal subgroup of G, then the quotient topology on G/H turns G/H into a topological group and the canonical epimorphism $G \to G/H$ will be continuous and open. Recall that the quotient topology is the finest topology on G/H such that $G \to G/H$ is continuous. If G admits a continuous open epimorphism f onto the topological group G_1, then its kernel H is a closed normal subgroup of G, and f induces a topological isomorphism between G/H and G_1. Note that if G is compact, then the epimorphism $f : G \to G_1$ is open already if it is continuous (cf. [PON]). Here, we shall prove this assertion under the assumption that in both groups G and G_1, the open normal subgroups of G form a basis for the neighborhood filter of 1 (which is always the case for profinite groups, as we will see later). It suffices to show that for every open normal subgroup H of G, its image $f(H)$ is an open subgroup of G_1. We know already that in compact topological groups, the open subgroups are precisely the closed subgroups of finite index. Hence, H is closed and thus compact, and since the continuous homomorphism f sends compact sets onto compact sets, also $f(H)$ is closed. On the other hand, $(G : H)$ is finite, and since f is an epimorphism, also $(G_1 : f(H))$ is finite. Therefore, $f(H)$ is an open subgroup of G_1 (in fact, it is also normal since f is an epimorphism). Note that under the same condition, a group homomorphism $f : G \to G_1$ is continuous already if for every open normal subgroup H_1 of G_1 there is an open normal subgroup H of G with $f(H) \subset H_1$.

Let H and N be closed subgroups of G. Then their intersection $H \cap N$ is again a closed subgroup of G. Their **group compositum** $H.N$ is defined to be the closure of the subgroup generated by H and N, i.e. the intersection of all closed subgroups containing H and N. If the topology on G is discrete, (which we will always assume if G is finite or no topology is

specified), then this compositum coincides with the subgroup generated by H and N. In contrast to "$H.N$", the notation HN indicates the set of products $\{h \cdot n \mid h \in H\,,\, n \in N\}$. If N is a normal subgroup of G, then $HN = NH$ and the group compositum $H.N$ is equal to HN. Further, if $H.N = G$ and $H \cap N = \{1\}$, then H is called a **group complement of N in G.**

Let H and N be closed subgroups of the compact topological group G. If N is normal in G, then there is a topological isomorphism between $H/(H \cap N)$ and HN/N. This is seen as follows. Let f be the restriction of the canonical epimorphism $HN \to HN/N$ to the subgroup H of HN. Then f is still continuous and surjective. Since H is compact, f is also open. Hence, it induces a topological isomorphism $H/\ker f \cong HN/N$. Since $\ker f = H \cap N$, this proves our assertion. Note that it is in general not true without the assertion that G be compact; for an example, see [BOU2], Chapter III, §2.7. In contrast to this, if H is also a normal subgroup and contains N, then G/H and $(G/N)/(H/N)$ are topologically isomorphic, even if G is not compact (cf. [BOU2], Chapter III, §2.7, Corollary to Proposition 22).

Let G be the inverse limit of an inverse system $\{G_i, \pi_{ji}\}$ of topological groups G_i. Since the topology on G is the coarsest such that all projections $\pi_i : G \to G_i$ are continuous, the maps $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ will be continuous on G if multiplication is defined componentwise. Hence, the inverse limit of an inverse system $\{G_i, \pi_{ji}\}$ of topological groups is again a topological group. Further, $\{1\} = \bigcap_i \pi_i^{-1}(1)$ is closed (since we have assumed that $\{1\}$ is closed in every G_i).

The inverse limit G of an inverse system of finite groups G_i (which are endowed with the discrete topology) is called a **profinite group**. By Lemma 24.7, G is hausdorff and compact. Therefore, for profinite groups all results hold that we stated for compact topological groups (with $\{1\}$ a closed subgroup). As we have noted in the last section, a basis for the topology of G is given by the sets $\pi_i^{-1}(\mathcal{U}_i)$ where $i \in I$ and $\mathcal{U}_i$ is an open subset of G_i. Since $\{g_i\}$ is open in G_i for every $g_i \in G_i$ and $\pi_i^{-1}(\mathcal{U}_i)$ is the union over all $\pi_i^{-1}(g_i)$ with $g_i \in \mathcal{U}_i$, we find that the sets $\pi_i^{-1}(g_i)$, $g_i \in G_i$, $i \in I$, form a basis of the topology on G. Since $\{g_i\}$ is also closed in G_i, the set $\pi_i^{-1}(g_i)$ is at the same time open and closed. If $g, h \in G$ and $g \neq h$, then there is $i \in I$ such that $\pi_i g \neq \pi_i h$ and consequently, g and h lie in the disjoint open and closed sets $\pi_i^{-1}(\pi_i g)$ and $\pi_i^{-1}(\pi_i h)$ respectively. This proves that the connected component of every $g \in G$ is just $\{g\}$, that is, G is **totally disconnected**.

The set $\pi_i^{-1}(1)$ is the kernel of the projection π_i, and thus it is an open normal subgroup of G. Since the sets $\pi_i^{-1}(g_i)$ form a basis of the topology, an open set containing 1 must contain at least one set of the form $\pi_i^{-1}(1)$. Consequently, the open normal subgroups of G form a basis for the neighborhood filter of $1 \in G$. Their intersection is $\{1\}$; indeed, for every $g \in G \setminus \{1\}$ there is some $i \in I$ such that $\pi_i g \neq 1 \in G_i$ and consequently, $g \notin \pi_i^{-1}(1)$.

Every closed subgroup H of G is equal to the intersection of all open subgroups containing H. This is seen as follows. Let $g \in G$ be an element which belongs to every open subgroup of G that contains H. For every open normal subgroup N of G, the group HN is closed, and since it contains N, it is also of finite index in G. Thus, HN is open. By assumption, $g \in HN$ and thus, $gN \cap H \neq \emptyset$. Since N and H are closed, so is $gN \cap H$. Since any finite intersection of open normal subgroups N_i is again an open normal subgroup N, any finite intersection $\bigcap_i (gN_i \cap H) = g \bigcap_i N_i \cap H = gN \cap H$ is nonempty. By compactness, the intersection of all of these sets, N running through all open normal subgroups of G, is nonempty. That is, there is some $h \in H$ such that $h \in gN$ for every such N. But the in-

tersection of all open normal subgroups N is $\{1\}$, showing that $g = h \in H$. This completes the proof. If in addition also H is normal, then every HN is normal and our argument shows that H is equal to the intersection of all open normal subgroups containing H.

Let N_i, $i \in I$, be a family of open normal subgroups of the profinite group G. The index set is partially ordered through $i \leq j \Leftrightarrow N_j \subset N_i$. If $i \leq j$, then we have the canonical epimorphism $\eta_{ji} : G/N_j \to G/N_i$. These projections satisfy properties (INV1) and (INV2). If the family contains *all* open normal subgroups of G, then also (INV0) holds, because then the family is a basis for the neighborhood filter of $1 \in G$. We ask whether we may identify G with $\varprojlim G/N_i$.

Lemma 24.8 *Let G be a compact topological group and let N_i, $i \in I$, be a family of open normal subgroups in G with the following properties:*

(1) the subgroups N_i form a basis for the neighborhood filter of 1,
(2) $\bigcap_{i\in I} N_i = \{1\}$.

Then the map $g \mapsto (gN_i)_{i\in I}$ is a topological isomorphism from G onto $\varprojlim G/N_i$, showing that G is a profinite group.

Proof: The canonical epimorphisms $G \to G/N_i$ are continuous. By the universal property of the product, the induced map $\iota : G \to \prod_{i\in I} G/N_i$ is continuous. The image of G lies in the subgroup $\varprojlim G/N_i$. If $g \neq 1$ then by condition (2) there is some N_i which does not contain g. Thus, $\iota g \neq 1$, showing that ι is injective. Let $(g_iN_i)_{i\in I}$ be an element in $\varprojlim G/N_i$. From condition (1) it follows that for every finite $J \subset I$ there is some $i \in I$ such that $N_i \subset \bigcap_{i\in J} N_j$. Then $g_iN_i \subset \bigcap_{j\in J} g_jN_j$, showing that the intersection is not empty. Since the sets g_iN_i are closed and G is compact, it follows that there exists $g \in \bigcap_{i\in I} g_iN_i$. This element satisfies $\iota g = (g_iN_i)_{i\in I}$. We have proved that ι is surjective. Condition (1) implies that the open normal subgroups of G form a basis for the neighborhood filter of 1. For groups with this property, we have shown that continuous epimorphisms are open. Hence ι is open and ι^{-1} is continuous. □

Corollary 24.9 *a) Every profinite group G is topologically isomorphic to $\varprojlim G/N_i$ where N_i runs through all open normal subgroups of G. That is, every profinite group is (up to topological isomorphism) the inverse limit of its finite quotients.*

b) Every closed subgroup of a profinite group G is again a profinite group.

c) If N is a closed normal subgroup of the profinite group G, then G/N is a profinite group.

Proof: a): This follows directly from the foregoing lemma since we have shown earlier that the intersection of all open normal subgroups of a profinite group G is $\{1\}$.

b): If H is a closed subgroup of a profinite group G, then H is compact. We take N_i, $i \in I$, to be all intersections of H with open normal subgroups of G. Since the open normal subgroups of G form a basis of the neighborhood filter of 1 and their intersection is $\{1\}$, the same is true for the open normal subgroups N_i in H. Now our assertion follows from the foregoing lemma, applied to H in the place of G.

c): N is the intersection of open normal subgroups N_i of G that contain N. The family N_i/N of open normal subgroups of G/N satisfies the conditions of the foregoing lemma and again, the assertion follows from that lemma, applied to G/N in the place of G. □

Every compact, hausdorff, totally disconnected topological group is a profinite group (and vice versa, as we have already shown). This is proved as follows. One shows that in a compact hausdorff group G, the connected component of $g \in G$ is equal to the intersection of all closed open neighborhoods of g (cf. [RIBES], Lemma 2.3). If G is also totally disconnected, then this intersection is $\{g\}$. Further, one shows that every closed open neighborhood of 1 contains an open normal subgroup (cf. [RIBES], Lemma 2.4). Hence, the open normal subgroups of G satisfy the conditions 1) and 2) of Lemma 24.8 and we obtain that G is indeed a profinite group.

For a collection of exercises on topological and profinite groups, see [FR–JA], at the end of Chapter 1.

24.4 Infinite Galois theory

We have already seen at the end of Section 24.2 that every Galois group $\operatorname{Gal} L|K$ is isomorphic to the inverse limit of the finite Galois groups $\operatorname{Gal} L_i|K$ where $L_i|K$ runs through all finite normal subextensions of $L|K$. (In fact, Lemma 24.8 shows that it is not necessary to take *all* of them; it suffices to take a family of subextensions of $L|K$ such that every finite normal subextension of $L|K$ is contained in some member of that family.) Taking all finite Galois groups to be endowed with the discrete topology, this representation of $\operatorname{Gal} L|K$ as an inverse limit of finite Galois groups turns $\operatorname{Gal} L|K$ into a profinite group, with projections $\pi_i = \operatorname{res}_{L_i}$. The induced topology on $\operatorname{Gal} L|K$ is called the **Krull topology**. Hence, Galois groups with the Krull topology have all properties that we have already stated for profinite groups and for compact topological groups (with $\{1\}$ a closed subgroup). Conversely, every profinite group is the Galois group of some Galois extension (cf. [FR–JA], Corollary 1.11).

A basis of the neighborhood filter of 1 is given by the subgroups $\operatorname{Gal} L|L_i = \operatorname{res}_{L_i}^{-1}(1)$ of $\operatorname{Gal} L|K$, where $L_i|K$ runs through all finite normal subextensions of $L|K$. (It follows from Theorem 24.10 below that these subgroups are precisely all open normal subgroups of $\operatorname{Gal} L|K$.) If $L|K$ is finite, then $\operatorname{Gal} L|K$ is a finite group and the Krull topology is discrete.

If $F|K$ is a finite subextension of $L|K$, then there exists $i \in I$ such that $F|K$ is a subextension of the finite normal subextension $L_i|K$. In this case, $\operatorname{Gal} L|F$ is an open and closed subgroup of $\operatorname{Gal} L|K$ since it coincides with the finite intersection of the open and closed sets $\operatorname{res}_{L_i}^{-1}(g_i)$ where the $g_i \in \operatorname{Gal} L_i|K$ run through all automorphisms of $L_i|K$ which fix every element of F. If $F|K$ is an arbitrary subextension of $L|K$, then it is the union of finite subextensions $F_j|K$ of $L|K$. Consequently, $\operatorname{Gal} L|F = \bigcap_j \operatorname{Gal} L|F_j$ is a closed subgroup of $\operatorname{Gal} L|K$.

Recall that the **closure** of a set S is the intersection of all closed sets containing S. Consequently, an element σ belongs to the closure of S if and only if for every open set U containing σ, the intersection $S \cap U$ is nonempty. For a profinite group G and $S \subset G$, this is the case if and only if for every open normal subgroup H of G, the intersection $S \cap \sigma H$ is nonempty (indeed, since the open subgroups H of G form a basis of the neighborhood

filter of 1, the sets σH form a basis of the neighborhood filter of σ). If $G = \mathrm{Gal}\, L|K$, then σ lies in the closure of S if and only if $S \cap \sigma \mathrm{Gal}\, L|L_i \neq \emptyset$ for every finite normal subextension $L_i|K$ of $L|K$. But $S \cap \sigma \mathrm{Gal}\, L|L_i \neq \emptyset$ just means that $\mathrm{res}_{L_i}(\sigma) \in \mathrm{res}_{L_i}(S)$. We have thus proved: *The closure of a set $S \subset \mathrm{Gal}\, L|K$ consists of all $\sigma \in \mathrm{Gal}\, L|K$ such that $\mathrm{res}_{L_i}(\sigma) \in \mathrm{res}_{L_i}(S)$ for every finite normal subextension $L_i|K$ of $L|K$.*

For every subgroup H of $\mathrm{Gal}\, L|K$, we let $\mathrm{Fix}\,(L, H)$ denote the **fixed field of H in L**, consisting of all elements of L which are fixed by all automorphisms in H. This fixed field is a subfield of L containing K.

Now we are ready to state the **Galois correspondence** for (not necessarily finite) Galois extensions. Note that the Krull topology on a finite profinite group is discrete, which yields that every subgroup is closed. So for finite Galois extensions, the following indeed gives the usual Galois correspondence.

Theorem 24.10 *Let $L|K$ be a Galois extension. The map $F \mapsto \mathrm{Gal}\, L|F$ is a bijection from the set of all subextensions $F|K$ of $L|K$ onto the set of all closed subgroups of $\mathrm{Gal}\, L|K$. Its inverse is the map $H \mapsto \mathrm{Fix}\,(L, H)$. For this correspondence, the following rules hold (where E, F are subfields of L containing K, the groups G, H are closed subgroups of $\mathrm{Gal}\, L|K$, and $\sigma \in \mathrm{Gal}\, L|K$):*

(Gal1) $E \subset F \Leftrightarrow \mathrm{Gal}\, L|E \supset \mathrm{Gal}\, L|F$

(Gal1′) $G \subset H \Leftrightarrow \mathrm{Fix}\,(L, G) \supset \mathrm{Fix}\,(L, H)$

(Gal2) $\mathrm{Gal}\, L|(E\,.\,F) = \mathrm{Gal}\, L|E \cap \mathrm{Gal}\, L|F$

(Gal3) $\mathrm{Gal}\, L|(E \cap F) = \mathrm{Gal}\, L|E\,.\,\mathrm{Gal}\, L|F$

(Gal2′) $\mathrm{Fix}\,(L, G \cap H) = \mathrm{Fix}\,(L, G)\,.\,\mathrm{Fix}\,(L, H)$

(Gal3′) $\mathrm{Fix}\,(L, G\,.\,H) = \mathrm{Fix}\,(L, G) \cap \mathrm{Fix}\,(L, H)$

(Gal4) $\mathrm{Gal}\, L|E$ *is a group complement of* $\mathrm{Gal}\, L|F$ *in* $\mathrm{Gal}\, L|K$ *if and only if E is a field complement of F in L over K.*

(Gal5) $\mathrm{Gal}\, L|\sigma E = \sigma(\mathrm{Gal}\, L|E)\sigma^{-1}$

(Gal5′) $\mathrm{Fix}\,(L, \sigma G \sigma^{-1}) = \sigma \mathrm{Fix}\,(L, G)$

(Gal6) $E|K$ *is a Galois extension if and only if* $\mathrm{Gal}\, L|E$ *is normal in* $\mathrm{Gal}\, L|K$.

Proof: For the proof of these assertions in the case of a finite Galois extension $L|K$, see [LANG3], Chapter VIII, §1. Note that (Gal4) follows from (Gal2), (Gal3), (Gal2′), (Gal3′), and that (Gal6) follows from (Gal5), (Gal5′).

Let $E|K$ be a subextension of $L|K$ and $G = \mathrm{Gal}\, L|E$. Then $E \subset \mathrm{Fix}\,(L, G)$. Let $a \in \mathrm{Fix}\,(L, G)$. Since $L|E$ is again a Galois extension, a is contained in a finite Galois subextension $M|E$ of $L|E$. Since every $\sigma \in \mathrm{Gal}\, M|E$ can be extended to an automorphism of $L|E$, we find that $\sigma a = a$ for every such σ. By finite Galois Theory, $a \in E$, showing that $E = \mathrm{Fix}\,(L, G)$.

Conversely, let G be an arbitrary subgroup of $\mathrm{Gal}\, L|K$ and $E = \mathrm{Fix}\,(L, G)$. Then $G \subset \mathrm{Gal}\, L|E$. We show that $\mathrm{Gal}\, L|E$ is equal to the closure of G; then $G = \mathrm{Gal}\, L|E$ if G is closed. Let $\sigma \in \mathrm{Gal}\, L|E$; we have to show that $\mathrm{res}_{L_i}(\sigma) \in \mathrm{res}_{L_i}(G) =: G_i$ for every finite normal subextension $L_i|K$ of $L|K$. Since E is the fixed field of G in L, we find that

E is also the fixed field of G_i in $E.L_i$. By finite Galois Theory, $G_i = \operatorname{Gal} E.L_i|E$. Hence, $\operatorname{res}_{L_i}(\sigma) \in G_i$.

The proof of all remaining assertions is left to the reader. □

Now let $L|K$ and $L'|K'$ be two Galois extensions such that $L \subset L'$ and $K \subset K'$. Then the restriction map $\operatorname{res}_L : \operatorname{Gal} L'|K' \to \operatorname{Gal} L|K$ is a group homomorphism. It is continuous (and hence open); indeed, if $L_i|K$ is a finite normal subextension of $L|K$, then also $L_i.K'|K'$ is a finite normal extension, and $\operatorname{res}_L(\operatorname{Gal} L'|L_i.K') \subset \operatorname{Gal} L|L_i$. Since K' is the fixed field of $\operatorname{Gal} L'|K'$ in L', we find that $L \cap K'$ is the fixed field of $\operatorname{res}_L(\operatorname{Gal} L'|K')$ in L. Further, $\operatorname{res}_L(\operatorname{Gal} L'|K')$ is compact and thus closed in $\operatorname{Gal} L|K$. From the foregoing theorem, we may now infer that $\operatorname{res}_L(\operatorname{Gal} L'|K') = \operatorname{Gal} L \,|\, L \cap K'$. We have proved that the restriction is in fact a continuous epimorphism

$$\operatorname{res}_L : \operatorname{Gal} L'|K' \longrightarrow \operatorname{Gal} L \,|\, L \cap K' .$$

Its kernel is $\operatorname{Gal} L'|L.K'$. Note that for every subextension $E'|K'$ of $L'|K'$, the fixed field of $\operatorname{res}_L(\operatorname{Gal} L'|E')$ in L is $E' \cap L$. Conversely, if E is this fixed field, then $E' = E.K'$.

Now we apply our results to two special cases. The first is the case of $K = K'$ and $L \subset L'$, that is, the restriction to a subextension. The second is the case of $L' = L.K'$ where the kernel is trivial and the above epimorphism is an isomorphism. We obtain:

Theorem 24.11 *Let $L|K$ be a Galois extension. Then:*

(Gal7) *If $E|K$ is a Galois subextension of $L|K$, then the restriction of the automorphisms of $L|K$ to E is a continuous open epimorphism with kernel $\operatorname{Gal} L|E$, giving rise to a topological isomorphism $\operatorname{Gal} E|K \cong \operatorname{Gal} L|K \,/\, \operatorname{Gal} L|E$. If $F|K$ is a subextension of $L|K$, then the fixed field of $\operatorname{res}_E(\operatorname{Gal} L|F)$ in E is $E \cap F$.*

(Gal8) *If $K'|K$ is an arbitrary field extension, then $L.K'|K'$ is a Galois extension, and the restriction of the automorphisms of $L.K'|K'$ to L is a continuous open epimorphism giving rise to a topological isomorphism $\operatorname{Gal} L.K'|K' \cong \operatorname{Gal} L \,|\, L \cap K'$. If $E|K$ and $E'|K'$ are subextensions of $L|K$ and $L.K'|K'$ respectively and if $\operatorname{Gal} L|E$ is the image of $\operatorname{Gal} L.K'|E'$ under this isomorphism, then $E = E' \cap K$ and $E' = E.K'$.*

(Gal9) *If $K'|K$ is a Galois extension, then $L.K'|K$ is a Galois extension and the restrictions of the automorphisms of $L.K' \,|\, L \cap K'$ to L and K' give a topological isomorphism $\operatorname{Gal} L.K' \,|\, L \cap K' \cong \operatorname{Gal} L \,|\, L \cap K' \times \operatorname{Gal} K' \,|\, L \cap K'$, where the latter is endowed with the product topology. Further,*

$$\operatorname{Gal} L.K'|K \cong \{(\sigma, \tau) \in \operatorname{Gal} L|K \times \operatorname{Gal} K'|K \mid \operatorname{res}_{L\cap K'}(\sigma) = \operatorname{res}_{L\cap K'}(\tau)\}.$$

The proof of (Gal9) uses (Gal7) and the following fact whose proof we leave to the reader: If N_1, N_2 are normal subgroups of G, then

$$G/(N_1 \cap N_2) \cong G/N_1 \times G/N_2 . \tag{24.2}$$

From (Gal7), where we replace K by $L \cap K'$, we obtain epimorphisms from $\operatorname{Gal} L.K'|L \cap K'$ onto $\operatorname{Gal} L|L \cap K'$ and $\operatorname{Gal} K'|L \cap K'$ with kernels $N_1 := \operatorname{Gal} L.K'|K'$ and $N_2 := \operatorname{Gal} L.K'|L$ respectively. But $N_1 \cap N_2 = \{1\}$, which yields (Gal9).

24.5 Linearly disjoint and algebraically disjoint extensions

Let $L|K$ and $F|K$ be subextensions of some extension Ω of the field K. **Unless stated otherwise, we always assume all fields to be contained in such a universal extension field Ω.** The elements $x_1, \ldots, x_n \in L$ are said to be **K-linearly independent** if $c_1x_1 + \ldots + c_nx_n = 0$ with $c_1, \ldots, c_n \in K$ implies that $c_i = 0$ for all i. In other words, $x_1, \ldots, x_n$ are K-linearly dependent if there exists a non-trivial K-linear combination $\sum c_ix_i$ which equates to zero. If $x_i \neq 0$, then $c_ix_i = 0$ implies $c_i = 0$, hence the x_i are K-linearly independent if and only if they are K-independent (where L is viewed as a K-module). We say that $L|K$ **is linearly disjoint from** $F|K$ **(in** Ω**)** if for every $n \in \mathbb{N}$ and every choice of K-linearly independent elements $x_1, \ldots, x_n \in L$, these elements will also be F-linearly independent. We shall show that this property is symmetrical, that is, it implies that for every $n \in \mathbb{N}$ and every choice of K-linearly independent elements $y_1, \ldots, y_n \in F$, these elements will also be L-linearly independent. Hence, assume that $L|K$ is linearly disjoint from $F|K$ and suppose that $y_1, \ldots, y_n \in F$ are K-linearly independent elements which satisfy a linear dependence relation

$$x_1y_1 + \ldots + x_ny_n = 0$$

where $x_i \in L$. Then our definition implies that the x_i must be K-linearly dependent. Without loss of generality, we may assume that there is $m < n$ such that $x_1, \ldots, x_m$ are K-linearly independent and that there are $c_{ij} \in K$ such that $x_i = \sum_{j=1}^{m} c_{ij}x_j$ for $m < i \leq n$. Then we may rewrite the dependence relation as follows:

$$\sum_{j=1}^{m} x_jy_j + \sum_{i=m+1}^{n} \left(\sum_{j=1}^{m} c_{ij}x_j \right) y_i = 0 \, .$$

Reorganizing the terms, we find

$$\sum_{j=1}^{m} \left(y_j + \sum_{i=m+1}^{n} c_{ij}y_i \right) x_j = 0 \, .$$

In this sum, the coefficient of every x_j is nonzero since the elements y_i were assumed to be K-linearly independent. Hence, the elements $x_1, \ldots, x_m$ are not F-linearly independent. On the other hand, $x_1, \ldots, x_m$ were assumed to be K-linearly independent, which contradicts our assumption that $L|K$ be linearly disjoint from $F|K$.

In view of the symmetry that we have just proved, we also say that L **and** F **are** K**-linearly disjoint** if $L|K$ is linearly disjoint from $F|K$. Note that if L and F are linearly disjoint over K, then also for arbitrary subextensions $L'|K$ of $L|K$ and $F'|K$ of $F|K$, the fields L' and F' are K-linearly disjoint.

Assume that $\mathcal{B}$ is a K-basis of L. If L and F are K-linearly disjoint, then the elements of $\mathcal{B}$ remain F-linearly independent, and consequently, $\mathcal{B}$ is also an F-basis of $L.F$. On the other hand, if the elements of $\mathcal{B}$ remain F-linearly independent, then also the basis of every finite K-subvector space of L will remain F-linearly independent, which implies that $L|K$ is linearly disjoint from $F|K$. Consequently,

$L|K$ is linearly disjoint from $F|K$ if and only if every finitely generated subextension of $L|K$ is linearly disjoint from $F|K$.

An algebraic extension $L|K$ is linearly disjoint from $F|K$ if and only if $[L' : K] = [L'.F : F]$ for every finite subextension $L'|K$.

A finite extension $L|K$ is linearly disjoint from $F|K$ if and only if $[L : K] = [L.F : F]$.

The proof of the following transitivity property is left to the reader; it can also be found in [LANG3], Chapter X, §5.

Lemma 24.12 *Let $L|K$ and $F \supset E \supset K$ be field extensions, all contained in the common extension field Ω. Then $L|K$ is linearly disjoint from $F|K$ if and only if $L|K$ is linearly disjoint from $E|K$ and $L.E|E$ is linearly disjoint from $F|E$.*

Lemma 24.13 *Let $F|K$ be an arbitrary extension with K relatively algebraically closed in F. Then $F|K$ is linearly disjoint from every simple algebraic and every separable algebraic extension of K. Moreover, if $L|K$ is separable algebraic, then L is relatively algebraically closed in $L.F$.*

Proof: Let $K(b)|K$ be algebraic. Then b is also algebraic over F. All conjugates of b (over K and hence also over F) are algebraic over K. The same is thus true for the coefficients of the minimal polynomial $f \in F[X]$ of b over F since they are symmetric functions in the conjugates of b over F. Since K is assumed to be relatively algebraically closed in F, it follows that $f \in K[X]$. Hence, f is also the minimal polynomial of b over K. Thus, $[F(b) : F] = [K(b) : K]$, showing that $F|K$ is linearly disjoint from $K(b)|K$.

Now let $L|K$ be a separable algebraic extension. Then every finite subextension of $L|K$ is simple and thus linearly disjoint from $F|K$. This proves that $L|K$ itself is linearly disjoint from $F|K$. Let $b \in L.F$ be algebraic over L. Since $L|K$ is separable algebraic, so is $L.F|F$. Hence, b is separable algebraic over F. But we have already shown that the minimal polynomial of b over F coincides with that over K. This shows that b is separable algebraic over K. Consequently, $L(b)|K$ is a separable extension. From what we have just proved, we thus know that $L(b)|K$ is linearly disjoint from $F|K$. By Lemma 24.12, $L(b)|L$ is linearly disjoint from $L.F|L$. In particular, $b \in L.F$ implies $b \in L$. This proves that L is relatively algebraically closed in $L.F$. □

Now assume that $L|K$ is a Galois extension and that it is not linearly disjoint from $F|K$. Since every finite Galois extension is simple, it follows that there is some $b \in L \setminus K$ such that the minimal polynomial f of b over K does not remain irreducible over F. Then the minimal polynomial h of b over F is a factor of f of smaller degree than f and consequently, not all of its coefficients will lie in K. On the other hand, these coefficients are elementary symmetric functions in the roots of h, and these roots are all in L since $L|K$ was assumed to be normal. Consequently, the coefficients of h lie in $L \cap F$, showing that this is a proper extension of K. Conversely, if $L \cap F$ is a proper extension of K, then L and F can not be K-linearly disjoint. We have proved:

Lemma 24.14 *Let $L|K$ a Galois and $F|K$ an arbitrary field extension. Then L and F are K-linearly disjoint if and only if $L \cap F = K$. More precisely, L and F are $(L \cap F)$-linearly disjoint.*

For a related criterion, see Lemma 24.34 below. From this Lemma together with (Gal8), we obtain:

Corollary 24.15 *Let $L|K$ be a Galois extension which is linearly disjoint from the arbitrary field extension $K'|K$. Then $L.K'|K'$ is a Galois extension, and the restriction of the automorphisms of $L.K'|K'$ to L is a topological isomorphism* $\operatorname{Gal} L.K'|K' \cong \operatorname{Gal} L|K$.

Let $L|K$ be any field extension. We say that $t_1, \ldots, t_n \in L$ are **K-algebraically independent** or **algebraically independent over** K if there is no non-trivial polynomial $f(X_1, \ldots, X_n)$ with coefficients in K such that $f(t_1, \ldots, t_n) = 0$. Infinitely many elements t_i , $i \in I$, are called K-algebraically independent if every finite subset of them is K-algebraically independent. A single element t is called **transcendental over** K if it is K-algebraically independent. The elements t_i , $i \in I$, are K-algebraically independent if and only if for every choice of elements a_i , $i \in I$, in some extension field of K there is (a uniquely determined) homomorphism from the ring $K[t_i \mid i \in I]$ onto the ring $K[a_i \mid i \in I]$ over K which sends t_i to a_i for every $i \in I$.

A **transcendence basis of** $L|K$ is a maximal set of elements of L which are K-algebraically independent. The cardinality of all transcendence bases of $L|K$ is equal; it is called the **transcendence degree** of $L|K$ and will be denoted by $\operatorname{trdeg} L|K$. From every set of generators of L over K, one can select a transcendence basis $\mathcal{T}$ of $L|K$; indeed, one may just take $\mathcal{T}$ to be a maximal K-algebraically independent subset, so all other generators and thus also L will be algebraic over $K(\mathcal{T})$. Consequently,

Lemma 24.16 *Every finitely generated field extension $K(x_1, \ldots, x_n)$ has finite transcendence degree $\leq n$. Every finitely generated field has finite transcendence degree over its prime field.*

If $\mathcal{T}$ is a transcendence basis of $L|K$ and $F|K$ is an arbitrary extension, then a transcendence basis of $L.F|F$ can be selected from $\mathcal{T}$. In particular, if $\operatorname{trdeg} L|K$ is finite, then

$$\operatorname{trdeg} L.F|F \leq \operatorname{trdeg} L|K \ .$$

Note that the transcendence degree is additive, that is,

$$\operatorname{trdeg} L|K = \operatorname{trdeg} L|K' + \operatorname{trdeg} K'|K$$

for arbitrary extensions $L|K'$ and $K'|K$. The proof of these facts and the basic properties of transcendence bases and transcendence degree can be found in [LANG3], Chapter X.

An extension field $K(t_1, \ldots, t_n)$ of K is called a **rational function field in n variables over** K if the elements $t_1, \ldots, t_n$ are K-algebraically independent. An extension field F of K is called an **algebraic function field in n variables over** K if it is a finite extension of a rational function field in n variables over K, or equivalently, if it is a finitely generated extension of K of transcendence degree n. We also speak of the **algebraic function field** $F|K$.

We will say that $L|K$ is **algebraically disjoint from** $F|K$ or **free from** $F|K$ (in their common extension field Ω) if for every $n \in \mathbb{N}$ and every choice of K-algebraically independent elements $t_1, \ldots, t_n \in L$, these elements will also be F-algebraically independent. Observe that $L|K$ is algebraically disjoint from $F|K$ if and only if every finitely generated subextension $E|K$ of $L|K$ satisfies $\operatorname{trdeg} E|K = \operatorname{trdeg} E.F|F$. Note that the elements $t_1, \ldots, t_n \in L$ are K-algebraically independent if and only if the elements $t_1^{\nu_1} \cdot \ldots \cdot t_n^{\nu_n} \in L$, $\nu_1, \ldots, \nu_n \in \mathbb{N}$, are K-linearly independent. This implies:

Lemma 24.17 *If $L|K$ is linearly disjoint from $F|K$, then it is algebraically disjoint from $F|K$. Conversely, if $t_i \in L$, $i \in I$, are F-algebraically independent, then $K(t_i \mid i \in I)|K$ is linearly disjoint from $F|K$. If $t_i \in L$, $i \in I$, are K-algebraically independent, then $K(t_i \mid i \in I)|K$ is linearly disjoint from $\tilde{K}|K$ and in particular, K is relatively algebraically closed in $K(t_i \mid i \in I)$.*

(For the proof of the last assertion, the reader may show that K-algebraically independent elements t_i are also $\tilde{K}$-algebraically independent.)

Like linear disjointness, also algebraic disjointness is symmetrical: Suppose that $F|K$ is not algebraically disjoint from $L|K$, i.e. there exist $t_1, \ldots, t_n \in F$ which are K-algebraically independent but not L-algebraically independent. Since a dependence relation only requires finitely many coefficients from L, there is a finitely generated subextension $E|K$ of $L|K$ such that $t_1, \ldots, t_n \in F$ are E-algebraically dependent. That is, $n + \operatorname{trdeg} E|K > \operatorname{trdeg} E(t_1, \ldots, t_n)|K$. In view of $E(t_1, \ldots, t_n) = E.K(t_1, \ldots, t_n)$, and because of $n = \operatorname{trdeg} K(t_1, \ldots, t_n)|K$, we find that $\operatorname{trdeg} E.K(t_1, \ldots, t_n)|K(t_1, \ldots, t_n) < \operatorname{trdeg} E|K$. Hence, $\operatorname{trdeg} E.F|F < \operatorname{trdeg} E|K$. That is, $L|K$ is not algebraically disjoint from $F|K$.

In view of the symmetry that we have just proved, we will also say that L **and** F **are** K**-algebraically disjoint** if $L|K$ is algebraically disjoint from $F|K$. Note that if L and F are K-algebraically disjoint, then also for arbitrary subextensions $L'|K$ of $L|K$ and $F'|K$ of $F|K$, the fields L' and F' are K-algebraically disjoint. We leave it to the reader to prove the following analogue to Lemma 24.12:

Lemma 24.18 *Let $L|K$ and $F \supset E \supset K$ be field extensions, all contained in the common extension field Ω. Then $L|K$ is algebraically disjoint from $F|K$ if and only if $L|K$ is algebraically disjoint from $E|K$ and $L.E|E$ is algebraically disjoint from $F|E$.*

Every two field extensions $L|K$ and $F|K$ can be embedded in a common overfield in such a way that their images are K-algebraically disjoint. Indeed, if t_i, $i \in I$, is a transcendence basis of $F|K$, then we choose L-algebraically independent elements t_i', $i \in I$, and define an embedding $K(t_i \mid i \in I) \to L(t_i' \mid i \in I)$ by $t_i \mapsto t_i'$. Since $F|K(t_i \mid i \in I)$ is algebraic, this embedding can be extended to an embedding of F in the algebraic closure of $L(t_i' \mid i \in I)$, and we are done. In contrast to this, it is not always possible to embed two given field extensions in a common overfield in such a way that their images are linearly disjoint. For example, if they are algebraic and not linearly disjoint, then this will remain true for every embedding. But in any case, we have shown that every two fields can be embedded in a common extension field, that is, that the theory of fields has the **amalgamation property**.

Lemma 24.19 *Let $L|K$ be an arbitrary subextension of $\Omega|K$ and let $K(\mathcal{T})|K$ be generated by a set $\mathcal{T} \subset \Omega$ of elements which are K-algebraically independent. If they are also L-algebraically independent, that is, if L and $K(\mathcal{T})$ are K-algebraically disjoint, and if K is relatively algebraically closed in L, then $K(\mathcal{T})$ is relatively algebraically closed in $L(\mathcal{T})$.*

Proof: Every element in $L(\mathcal{T})$ algebraic over $K(\mathcal{T})$ is already algebraic over $K(\mathcal{T}_0)$ for a suitable finite subset $\mathcal{T}_0$ of $\mathcal{T}$. Hence, it suffices to prove the assertion in the case of $\mathcal{T}$ finite. Induction on the number of elements of $\mathcal{T}$ shows that it suffices to prove the assertion in the case of $\mathcal{T}$ consisting of just one element t. Let $r(t) = cf(t)/g(t) \in L(t)$,

with $c \in L$, $f(t), g(t) \in L[t]$ monic and f prime to g. If $r(t)$ is algebraic over $K(t)$, then there is an equation

$$h_n(t)r(t)^n + \ldots + h_0(t) = 0 \quad \text{with } h_i(t) \in K[t] \text{ and } h_0(t) \neq 0$$

such that $h_n(t), \ldots, h_0(t)$ have no common factor $\in K[t] \setminus K$. Multiplying by $g(t)^n$, we obtain

$$h_n(t)c^n f(t)^n + \ldots + h_0(t)g(t)^n = 0 \; .$$

Since t is transcendental over L, we can substitute for it an arbitrary root $b \in \tilde{L}$ of f to obtain that $h_0(b)g(b)^n = 0$. Since f was assumed to be prime to g, we have $g(b) \neq 0$. Hence, $h_0(b) = 0$, which shows that every root of f is algebraic over K. Consequently, the coefficients of the monic polynomial f, being symmetric functions in the roots, are all algebraic over K. Since K is assumed to be relatively algebraically closed in L, it follows that $f(t) \in K[t]$. By a similar argument, it is shown that $g(t) \in K[t]$.

Further, we substitute for t a root $d \in \tilde{L}$ of $f - g$ in the above equation. With this choice, we have $f(d) = g(d) \neq 0$ (f being prime to g), and we obtain that

$$h_n(d)c^n + \ldots + h_0(d) = 0 \; .$$

Since $h_n(t), \ldots, h_0(t)$ have no common non-trivial factor, not all $h_i(d)$ can be zero. Then at least two of the $h_i(d)$ are nonzero. This shows c to be algebraic over K and thus to be an element of K. Altogether, we find that $r(t) \in K(t)$. □

Lemma 24.20 *Suppose that L and F are K-algebraically disjoint. If for every finitely generated subextension $E|K$ of $F|K$, E is relatively algebraically closed in $E.L$, then L and F are K-linearly disjoint.*

Proof: It suffices to show that $L|K$ is linearly disjoint from every finitely generated subextension $K(x_1, \ldots, x_n)|K$ of $F|K$. Suppose that we have already shown that L and $K' := K(x_1, \ldots, x_{i-1})$ are K-linearly disjoint, for some $i \leq n$. In view of Lemma 24.12, it suffices to prove that $L' := L(x_1, \ldots, x_{i-1})$ and $K(x_1, \ldots, x_i)$ are K'-linearly disjoint. By hypothesis, K' is relatively algebraically closed in L'. If x_i is algebraic over K' then in view of Lemma 24.13, we are done. So assume that x_i is transcendental over K'. Then by our assumption that L and F are K-algebraically disjoint, it follows that x_i is also transcendental over L'. In this case, we are done by virtue of Lemma 24.17. □

24.6 Supernatural numbers

The degree $[L : K]$ of a finite field extension $L|K$ gives information about the degrees of all possible subextensions; these degrees are just divisors of $[L : K]$. Analogous information is contained in the order of a finite group, or the finite index of a subgroup. If we would just set $[L : K] = \infty$ if $L|K$ is infinite, then we would loose this information. In the case of infinite algebraic field extensions (and analogously, of profinite groups), we would like to generalize the notion of degree (resp., of order and index) in a way that preserves the

information of the finite case. To this end, we define a **supernatural number** to be a formal product

$$\mathbf{n} = \prod_{p \text{ prime}} p^{\mathbf{n}_p} \quad \text{with } \mathbf{n}_p \in \mathbb{N} \cup \{0, \infty\}$$

and define the product of two supernatural numbers $\mathbf{m}$, $\mathbf{n}$ by

$$\mathbf{m} \cdot \mathbf{n} = \prod_{p \text{ prime}} p^{\mathbf{m}_p + \mathbf{n}_p}$$

with the provision that $n + \infty = \infty + n = \infty + \infty = \infty$ for all $n \in \mathbb{N} \cup \{0\}$. Every natural number $n \neq 0$ can be viewed as a supernatural number $\mathbf{n}$ in a canonical way, taking $\mathbf{n}_p = v_p n$, where v_p denotes the usual p-adic valuation. A supernatural number $\mathbf{n}$ is said to be a **power of** p if it is of the form p^ν with $\nu \in \mathbb{N} \cup \{0, \infty\}$.

If $\mathbf{m}$, $\mathbf{n}$ are supernatural numbers, then like for natural numbers, we will say that $\mathbf{m}$ **divides** $\mathbf{n}$, denoted by $\mathbf{m}|\mathbf{n}$, if there is a supernatural number ℓ such that $\mathbf{m} = \ell \cdot \mathbf{n}$. Hence, $\mathbf{m}$ divides $\mathbf{n}$ if and only if $\mathbf{m}_p \leq \mathbf{n}_p$ for all primes p. As for natural numbers, $\mathbf{m}|\mathbf{n} \wedge \mathbf{n}|\mathbf{m}$ implies $\mathbf{m} = \mathbf{n}$.

Observe that every subset of $\mathbb{N} \cup \{0, \infty\}$ has a supremum in $\mathbb{N} \cup \{0, \infty\}$. This gives us the possibility of defining the **least common multiple** of an arbitrary set $\mathcal{N}$ of supernatural numbers to be the supernatural number $\operatorname{lcm} \mathcal{N}$ given by

$$\operatorname{lcm} \mathcal{N} = \prod_{p}^{p^{\mathcal{N}_p}} \quad \text{with} \quad \mathcal{N}_p = \sup\{\mathbf{n}_p \mid \mathbf{n} \in \mathcal{N}\} ,$$

where p runs over all primes. It is clear from this definition that every $\mathbf{n} \in \mathcal{N}$ divides $\operatorname{lcm} \mathcal{N}$ and that this does not remain true if we replace $\operatorname{lcm} \mathcal{N}$ by any of its proper divisors. Note that it is the notion of a supernatural number that enables us to define a least common multiple for every infinite set of natural numbers. Similarly, the **greatest common divisor** $\gcd \mathcal{N}$ is defined by just replacing the supremum by the minimum. Then $\gcd \mathcal{N}$ divides every $\mathbf{n} \in \mathcal{N}$, but no proper multiple of $\gcd \mathcal{N}$ has this property. If $\mathcal{N} = \{\mathbf{m}, \mathbf{n}\}$, then we write $(\mathbf{m}, \mathbf{n})$ instead of $\gcd \mathcal{N}$. We say that $\mathbf{m}$ **is prime to** $\mathbf{n}$ if $(\mathbf{m}, \mathbf{n}) = 1$.

Now let $L|K$ be an algebraic field extension. Then we define

$$[L : K] := \operatorname{lcm} \{[E : K] \mid E|K \text{ a finite subextension of } L|K\} .$$

In the case of $L|K$ a finite extension, this coincides with the usual degree (just because $[E : K]$ is a divisor of $[L : K]$ for every subextension $E|K$).

If $L|K$ is an algebraic extension, linearly disjoint from the arbitrary extension $F|K$, then it follows from the definition of linear disjointness that $[L.F : F] = [L : K]$. But the converse is not true, if $L|K$ is not finite.

Lemma 24.21 *If $L|K$ is an algebraic extension and $K'|K$ a subextension of $L|K$, then*

$$[L : K] = [L : K'] \cdot [K' : K] .$$

Proof: In Section 24.1 we have shown that for every finite subextension $L_i'|K'$ of $L|K'$ there is a finite subextension $K_i|K$ of $K'|K$ and a finite subextension $L_i|K_i$ of $L|K_i$ such

that $L_i' = L_i.K'$ and $[L_i : K_i] = [L_i' : K']$. Moreover, $K_i|K$ may be chosen as to contain a given arbitrary finite subextension of $K'|K$. We have

$$[L_i' : K'] \cdot [K_i : K] = [L_i : K_i] \cdot [K_i : K] = [L_i : K] \tag{24.3}$$

with $L_i|K$ a finite subextension of $L|K$. It follows that for every finite subextension $L_i'|K'$ of $L|K'$ and $K_i|K$ of $K'|K$, the product $[L_i' : K'][K_i : K]$ divides $[L : K]$. Consequently, $[L : K'][K' : K]$ divides $[L : K]$.

For the converse, let $E|K$ be a finite subextension of $L|K$. We set $L_i' := E.K'$ and choose K_i and L_i as above. Recall that these both fields may be chosen such that L_i contains E. Hence, $[E : K]$ divides $[L_i : K]$. In view of (24.3), this in turn divides $[L : K'][K' : K]$. Hence, $[L : K]$ divides $[L : K'][K' : K]$. □

Now let G be a profinite group and H a closed subgroup of G. Then we define the **index of H in G** to be

$$(G : H) := \operatorname{lcm} \{(G : HN) \mid N \text{ an open normal subgroup of } G\} .$$

(Note that HN is of finite index in G since already N is.) Further, we define the **order of G** to be $\#G := (G : 1)$. Hence,

$$\#G = \operatorname{lcm} \{(G : N) \mid N \text{ an open normal subgroup of } G\} .$$

If G is finite, then 1 is an open normal subgroup of G, and $\#G$ coincides with the usual order. If $(G : H)$ is finite, then H is an open subgroup of G, and there is an open normal subgroup $N \subset H$ of G, showing that $(G : H)$ coincides with the usual index.

Lemma 24.22 *Let G be a profinite group and $H \subset \mathcal{H}$ closed subgroups of G. Then*

$$(G : H) = (G : \mathcal{H}) \cdot (\mathcal{H} : H) .$$

Proof: In what follows, let N always run through all open normal subgroups of G. Then the groups $H \cap N$ form a basis of the open normal subgroups of H. We compute: $(G : H) = \operatorname{lcm}_N(G : HN) = \operatorname{lcm}_N(G : \mathcal{H}N)(\mathcal{H}N : HN) = \operatorname{lcm}_N(G : \mathcal{H}N)(\mathcal{H}N/N : HN/N) = \operatorname{lcm}_N(G : \mathcal{H}N)(\mathcal{H}/\mathcal{H} \cap N : H(\mathcal{H} \cap N)/\mathcal{H} \cap N) = \operatorname{lcm}_N(G : \mathcal{H}N)(\mathcal{H} : H(\mathcal{H} \cap N))$. Since the intersection of any two open normal subgroups of G is again an open normal subgroup of G, the latter is equal to $\operatorname{lcm}_N(G : \mathcal{H}N) \cdot \operatorname{lcm}_N(\mathcal{H} : H(\mathcal{H} \cap N)) = (G : \mathcal{H})(\mathcal{H} : H)$. □

This lemma can also be deduced from Lemma 24.21, using the fact that every profinite group is the Galois group of a Galois extension, together with the following lemma:

Lemma 24.23 *Let $L|K$ be a Galois extension. Then*

$$[L : K] = \#\mathrm{Gal}\, L|K .$$

The finite case of this assertion is proved in finite Galois Theory. The infinite case follows from the definitions of $[L : K]$ and $\#\mathrm{Gal}\, L|K$ by Galois correspondence (Theorem 24.10).

If A is an abelian torsion group, then $\#A$ is defined to be

$$\#A := \operatorname{lcm} \{\#B \mid B \text{ a finite subgroup of } A\} .$$

Again, if A is finite, then this coincides with the usual order. To give an example,

$$\#\mathbb{Q}/\mathbb{Z} = \prod_{p \text{ prime}} p^\infty \ .$$

For further information and examples for supernatural numbers, see Chapter I, §4 of [RIBES].

Exercise 24.2 *Define the product over arbitrary sets of supernatural numbers. Use this to compute the order of direct products of abelian torsion groups.*

Exercise 24.3 *Show that* $(G : H) = \operatorname{lcm}\{(G : N) \mid N \text{ an open subgroup of } G \text{ containing } H\}$.

24.7 Separable and inseparable extensions

A field K is called **perfect** if every of its algebraic extensions is separable. By virtue of Lemma 24.3, this is the case if and only if the extension $\tilde{K}|K$ is separable. If $L|K$ is an algebraic extension, then $\tilde{K} = \tilde{L}$, and if $\tilde{L}|K$ is separable, then by Lemma 24.3, also $\tilde{L}|L$ is separable. The latter yields that L is perfect. Hence,

Lemma 24.24 *Every algebraic extension field of a perfect field is again perfect.*

The **characteristic exponent** of a field K is defined to be equal to the characteristic $\operatorname{char} K$ if this is nonzero (and hence a prime number), and to be equal to 1 otherwise. We will denote it by $\operatorname{charexp} K$. Let $p \geq 1$ be the characteristic exponent of K. Then K admits an injective endomorphism

$$\begin{array}{rccl} \varphi : & K & \to & K^p = \{a^p \mid a \in K\} \subset K \\ & a & \mapsto & a^p \ . \end{array}$$

(Recall that the binomial coefficients $\binom{p}{i}$ are divisible by p if and only if $1 \leq i \leq p-1$ or $p = 1$. In a field of characteristic $p > 0$ this just means that they vanish, showing that $(a+b)^p = a^p + b^p$, which proves the additivity of φ.) The endomorphism φ is called the **Frobenius endomorphism** or just **Frobenius of** K. It is surjective if and only if $K = K^p$. If $K = K^p$ holds, then one shows by induction that $K = K^{p^m}$ for all $m \geq 0$. Let us consider the Frobenius of the rational function field $\tilde{K}(X)$. Its restriction to the polynomial ring $\tilde{K}[X]$ is an endomorphism of $\tilde{K}[X]$. We have $(X-b)^{p^m} = X^{p^m} - b^{p^m}$ for every $b \in \tilde{K}$ and every $m \in \mathbb{N}$. We see that for every $a = b^{p^m} \in K$, the minimal polynomial $X^{p^m} - a$ of b over K admits only b as a root. That is, for every $a \in K$ there is a *unique* p^m-th root in $\tilde{K}$; we shall denote it by a^{1/p^m} or $a^{p^{-m}}$. We define K^{1/p^∞} to be the smallest algebraic extension field of K on which the Frobenius is surjective. It consists of all elements of $\tilde{K}$ which are a p^m-th root of some element in K, for some $m \in \mathbb{N}$; this collection of elements is indeed a field, as follows from the fact that the Frobenius (on $\tilde{K}$) is a homomorphism. Similarly, we obtain a field if we collect all elements of $\tilde{K}$ which are a p^m-th root of some element in K, for fixed m; this field is denoted by K^{1/p^m}. Note that K^{1/p^∞} is the union over all K^{1/p^m}, $n \in \mathbb{N}$, because for every element b in K^{1/p^∞} there is some integer $m \in \mathbb{N}$ such that $b^{p^m} \in K$. Observe that for an extension generated over K by the elements x_i, $i \in I$, we have

$$\begin{aligned} K(x_i \mid i \in I)^{1/p^m} &= K^{1/p^m}(x_i^{1/p^m} \mid i \in I) \ , \\ K(x_i \mid i \in I)^{p^m} &= K^{p^m}(x_i^{p^m} \mid i \in I) \ . \end{aligned}$$

Let $b \in \tilde{K}$ and f its minimal polynomial over K. We write $f = X^n + c_{n-1}X^{n-1} + \ldots + c_1X + c_0$ where the c_i are elements of K. Assume that for $i = 0, \ldots, n-1$, the index i is divisible by p if $c_i \neq 0$. Then f may be written in the form $f = g^p$ where $g = X^{n/p} + c_{n-p}^{1/p}X^{n/p-1} + \ldots + c_0^{1/p} \in K^{1/p}[X]$. In this case, every root of g occurs p-times as a root of f, showing that f is not separable, and b is not separable over K. Conversely, it can be shown that if f is not separable, then it is of the form $f = g^p$ with $g \in K^{1/p}[X]$. (In short, the proof is as follows. Since f has multiple roots, it has a root in common with its derivative $f' \in K[X]$. If f' does not vanish identically, it then follows that both f and f' have a common factor in $K[X]$, which is consequently of smaller degree than f. But this is a contradiction to the irreducibility of f. Consequently, $f' \equiv 0$ which can only be the case if $f = g^p$ with $g \in K^{1/p}[X]$.) Now if $K = K^p$, then all coefficients of g lie in K, which means that $g \in K[X]$, contradicting the irreducibility of f. This shows that if $K = K^p$, then every irreducible polynomial over K is separable. In particular, *every field of characteristic 0 is perfect.* On the other hand, if $K \neq K^p$, then there is some $a \in K$ such that $X^p - a$ is irreducible and not separable. We have proved:

Lemma 24.25 *The field K is perfect if and only if $K = K^p$, that is, if and only if the Frobenius is surjective. This in turn is equivalent to $K = K^{1/p^\infty}$.*

If L is a perfect extension field of K, then $L = L^{1/p^\infty}$ and thus, L contains K^{1/p^∞}. Since K^{1/p^∞} is perfect, it is consequently the smallest perfect extension field of K. Therefore, it is called the **perfect hull of** K.

If the polynomial $X^p - a$ is not irreducible over K, then it splits into linear factors. (Indeed, $X^p - a = (X - a^{1/p})^p$, and if $(X - a^{1/p})^n \in K[X]$ with $1 < n < p$, hence $a^{n/p} \in K$, then we choose integers r, s such that $rn + sp = 1$ and obtain that $a^{1/p} = (a^{n/p})^r \cdot a^s \in K$.) Hence, $[K(a^{1/p}) : K]$ is equal to p or to 1. It follows that $[K^{1/p} : K]$ and $[K^{1/p^\infty} : K]$ are powers of p. The reader may show that $[K^{1/p^\infty} : K] = p^\infty$ if K is not perfect.

Since the Frobenius is injective, it is an automorphism on every finite field; this shows that *every finite field is perfect.* Recall that for every power $q = p^m$ of p, there is precisely one finite field $\mathbb{F}_q$ with q elements and that for every n it admits precisely one extension of degree n, namely the field with p^{mn} elements. Every such extension is Galois, the Galois group being generated by φ^m (m is the smallest integer ≥ 1 such that φ^m fixes $\mathbb{F}_q$). For the proofs, see [LANG3], VII, §5, Theorems 10, 12 and 13).

Let $\sigma : K \to F$ be any embedding. The reader may show that σ admits an extension to an embedding $\tilde{\sigma} : \tilde{K} \to \tilde{F}$. For every subextension $E|K$ of $K^{1/p^\infty}|K$, there is a unique extension to an embedding $\sigma_E : E \to F^{1/p^\infty}$. Indeed, since for every $b \in K^{1/p^\infty}$ there is some $m \in \mathbb{N}$ such that $a := b^{p^m} \in K$, the extension σ_1 must satisfy $\sigma_1 b = (\sigma a)^{1/p^m}$. In particular, the only embedding of E in $\tilde{K}$ over K is the identity. Recall that an extension $E|K$ is called **purely inseparable** if it is algebraic and the only embedding of E in $\tilde{K}$ over K is the identity. If an extension is separable and purely inseparable, then it is trivial. Further, if $K \subset E \subset L$, then $L|K$ is purely inseparable if and only if $L|E$ and $E|K$ are. If $E|K$ is a purely inseparable subextension of a normal extension $L|K$, then every automorphism of $L|K$ will also fix E, hence we can identify $\operatorname{Gal} L|K$ and $\operatorname{Gal} L|E$. All subextensions of $K^{1/p^\infty}|K$ are purely inseparable. We are going to show that also the converse is true, that is, that every purely inseparable extension $E|K$ is a subextension of $K^{1/p^\infty}|K$.

Let f be an irreducible polynomial over K with coefficients $c_i \in K$. Choose p^m to be the highest power of p which divides all i for which $c_i \neq 0$. Then we can write $f = g^{p^m}$ with

$g(X) = \sum_j d_j X^j \in K^{1/p^m}[X]$ such that $c_i = d_j^{p^m}$ for $i = jp^m$. Note that g is irreducible over K^{1/p^m}, because every factorization $g = g_1 g_2$ yields a factorization $f = g_1^{p^m} g_2^{p^m}$, but f is irreducible by assumption. By our choice of m, there is some j not divisible by p such that $d_j \neq 0$. Consequently, g is separable over K^{1/p^m}. Observe that $m > 0$ if and only if f is not separable over K. On the other hand, we can also write $f = h(X^{p^m})$ where $h(X) = \sum_{j=1}^n c_{jp^m}(X) \in K[X]$. Then h is irreducible over K since every non-trivial factorization of h would also be a non-trivial factorization of f. If $a_1, \ldots, a_n$ are the roots of g in $\tilde{K}$, then they are all distinct because g is irreducible and separable over K^{1/p^m}. The Frobenius being injective, also $a_1^{p^m}, \ldots, a_n^{p^m}$ are all distinct. But these are the roots of h since $h(X^{p^m}) = f(X) = g(X)^{p^m} = \prod_{i=1}^n (X - a_i)^{p^m} = \prod_{i=1}^n (X^{p^m} - a_i^{p^m})$. This proves that also h is separable over K. We summarize:

Lemma 24.26 *Let $f \in K[X]$ be irreducible over K and p be the characteristic exponent of K. Then there is some integer $m \geq 0$ and $g \in K^{1/p^m}[X]$, irreducible over K^{1/p^m}, such that $f = g^{p^m}$. So if $a_1, \ldots, a_n$ are the roots of g in $\tilde{K}$, then they are all distinct, and*

$$f = g^{p^m} = \prod_{i=1}^n (X - a_i)^{p^m} = \prod_{i=1}^n (X^{p^m} - a_i^{p^m}) = h(X^{p^m})$$

with $h \in K[X]$ irreducible and separable over K. We have $\deg g = \deg h$ and $\deg f = p^m \deg g$. Further, f is separable over K if and only if $m = 0$.

Now let $E|K$ be purely inseparable. Let $b \in E$ and f its minimal polynomial over K. We write $f = g^{p^m}$ according to the foregoing lemma. Then g must be linear. Indeed, if g would admit at least two roots a_1, a_2, they would be distinct and one of them, say a_1, would be equal to b. Then the assignment $a_1 \mapsto a_2$ would induce an embedding of $K(b)$ in $\tilde{K}$ over K which is not the identity. Since it can be extended to an embedding of E in $\tilde{K}$ over K, this contradicts our assumption that $E|K$ be purely inseparable. This proves that g and thus also h is linear. But that means that $h(X) = X - b^{p^m}$ with $b^{p^m} \in K$. We have shown that for every $b \in E$, there is some integer $m \geq 0$ such that $b^{p^m} \in K$. That is, $E \subset K^{1/p^\infty}$. We have proved:

Lemma 24.27 *Let K be a field with characteristic exponent p. Then every purely inseparable extension $E|K$ is a subextension of $K^{1/p^\infty}|K$. In this sense, $K^{1/p^\infty}|K$ is the maximal purely inseparable extension of K. In particular, the compositum of two purely inseparable extensions of K is again a purely inseparable extension of K.*

If $E|K$ is a purely inseparable extension and $F|K$ is an arbitrary extension, then $E.F|F$ is again a purely inseparable extension, because it is contained in F^{1/p^∞}. Together with an earlier observation, this lemma also shows that

Lemma 24.28 *A given embedding of K in an arbitrary perfect field has a unique extension to every purely inseparable extension of K.*

Recall that an element $b \in \tilde{K}$ is called **purely inseparable over** K, if all roots in $\tilde{K}$ of its minimal polynomial over K are equal. The deduction of the above lemma has shown that b is purely inseparable over K if and only if $b \in K^{1/p^\infty}$. Hence, the lemma shows that an extension of K is purely inseparable if and only if it is generated by elements which are purely inseparable over K. If b is purely inseparable of degree p^m over K, then $b^{p^{m-1}}$ is purely inseparable of degree p over K, and b is purely inseparable of degree p^{m-1} over $K(b^{p^{m-1}})$. By induction, we obtain

Corollary 24.29 *Every finite purely inseparable extension is a tower of purely inseparable extensions of degree p.*

The maximal purely inseparable extension of an algebraic extension $L|K$ will be denoted by $(L|K)^{\text{ins}}$. By what we have shown, $K^{1/p^\infty} = (\tilde{K}|K)^{\text{ins}}$ and $(L|K)^{\text{ins}} = L \cap K^{1/p^\infty}$.

Let $L|K$ be an algebraic extension, $b \in \tilde{K}$ with minimal polynomial f over K, and let g be as in Lemma 24.26. If f is not separable over K, then the degree of g is smaller than that of f, which shows that $K(b)|K$ is not linearly disjoint from $K^{1/p^\infty}|K$. Therefore, if an algebraic extension $L|K$ is linearly disjoint from $K^{1/p^\infty}|K$, then each of its simple subextensions is separable and hence, $L|K$ is itself separable. To show the converse, assume that $K(b)|K$ is separable, that is, $K(b)$ has $[K(b) : K]$ distinct embeddings in $\tilde{K}$ over K. They extend to $[K(b) : K]$ distinct embeddings of $K(b).K^{1/p^\infty} = K^{1/p^\infty}(b)$ in $\tilde{K} = \widetilde{K^{1/p^\infty}}$ over K. But these embeddings are in fact embeddings over K^{1/p^∞} since they must be the identity on K^{1/p^∞}. This proves that $[K^{1/p^\infty}(b) : K^{1/p^\infty}] = [K(b) : K]$, showing that $K(b)$ and K^{1/p^∞} are K-linearly disjoint. In view of Lemma 24.27, we conclude:

Lemma 24.30 *Let $L|K$ be an algebraic extension. Then $L|K$ is separable if and only if it is linearly disjoint from $K^{1/p^\infty}|K$, and this holds if and only if $L|K$ is linearly disjoint from every purely inseparable extension of K.*

The degree $[K^{1/p} : K]$ of the purely inseparable extension $K^{1/p}|K$ is called the **p-degree of K**. It is equal to 1 if and only if K is perfect. Since φ is an endomorphism of $K^{1/p}$ with image K and an endomorphism of K with image K^p, the p-degree of K is equal to $[K : K^p]$. A basis of $K|K^p$ is called a **p-basis of K**. Note that φ^n sends a p-basis of K^{1/p^n} onto a p-basis of K, and it follows that the p-degree of K^{1/p^n} is equal to that of K.

Remark 24.31 Among model theoretic algebraists, the p-degree is also called **Ershov-invariant**. In the literature, it is usual that n is called the p-degree if $[K : K^p] = p^n$. This is the additive form of the p-degree. But for our purposes, the multiplicative notation has turned out to be more useful.

Lemma 24.32 *If $L|K$ is a separable algebraic extension, then $L^{1/p} = L.K^{1/p}$, and the p-degree of L is equal to that of K. If $L|K$ is an arbitrary finite extension, then again, the p-degree of L is equal to that of K.*

Proof: Let $\mathcal{B}$ be a basis of L over K. We know already that $L^{1/p} = K^{1/p}(b^{1/p} \mid b \in \mathcal{B})$.

Assume that $L|K$ is separable. Then for every $b \in \mathcal{B}$, we have $K(b) = K(b^p)$ since otherwise, the separable extension $K(b)|K$ would contain a non-trivial purely inseparable extension $K(b)|K(b^p)$, which is impossible. It follows that $L = K(\mathcal{B}) = K(b^p \mid b \in \mathcal{B})$, which gives $L^{1/p} = K^{1/p}(\mathcal{B}) = L.K^{1/p}$. Since L and $K^{1/p}$ are K-linearly disjoint, $L|K$ being separable, it now follows that $[L^{1/p} : L] = [K^{1/p} : K]$.

To prove our last assertion, assume now that $L|K$ is an arbitrary finite extension. We have that $[L^{1/p} : K^{1/p}][K^{1/p} : K] = [L^{1/p} : K] = [L^{1/p} : L][L : K]$. The Frobenius endomorphism sends $L^{1/p}$ onto L and $K^{1/p}$ onto K. Thus, $[L^{1/p} : K^{1/p}] = [L : K] < \infty$. If $[K^{1/p} : K]$ is finite, then this yields that $[K^{1/p} : K] = [L^{1/p} : L]$. If $[K^{1/p} : K]$ is infinite, then so is $[L^{1/p} : L]$, so both are equal to p^∞. □

Lemma 24.33 *If $L|K$ is an algebraic extension, then $[L : L^p] \leq [K : K^p]$.*

Proof: In view of the foregoing lemma, it suffices to prove our assertion in the case of a purely inseparable extension $L|K$. Assume first that both $[L : L^p]$ and $[K : K^p]$ are infinite cardinals. Then $[L : L^p]$ is equal to $[L^{1/p^\infty} : L]$ since $L^{1/p^\infty} = \bigcup_{I=1}^{\infty} L^{1/p^i}$ and $[L^{1/p^i} : L^{1/p^{i-1}}] = [L : L^p]$ for all i. The same holds for $[K : K^p]$, and in view of $L^{1/p^\infty} = K^{1/p^\infty}$, we obtain that $[L : L^p] = [L^{1/p^\infty} : L] \leq [K^{1/p^\infty} : K] = [K : K^p]$.

If $[K : K^p]$ is infinite and $[L : L^p]$ is finite, then there is nothing to prove. Now assume that $[K : K^p]$ is finite. Let $b_1, \ldots, b_n \in L^{1/p}$ be L-linearly independent. We set $E := K(b_1^p, \ldots, b_n^p) \subset L$. Then the elements $b_1, \ldots, b_n$ are also E-linearly independent, and they lie in $E^{1/p}$. But they are also algebraic over K and thus, $E|K$ is a finite extension. By the foregoing lemma, we find that $n \leq [K : K^p]$. This proves that $[L : L^p] \leq [K : K^p]$. $\square$

If K is not perfect, then it can happen that the p-degree drops under infinite inseparable algebraic extensions, as the extension $K^{1/p^\infty}|K$ shows.

Let us now discuss the behaviour of the p-degree under transcendental extensions. Let t_i, $i \in I$, be K-algebraically independent. Then also the elements $t_i^{p^m}$, $i \in I$, are K-algebraically independent, for every m. But also the elements t_i^{1/p^m}, $i \in I$, are K-algebraically independent, for every m. (Indeed, a non-trivial algebraic dependence relation of them could be raised to the p^m-th power to obtain a non-trivial algebraic dependence relation of the elements t_i.)

The finite products $\prod_{i \in I} t_i^{\nu_i}$ with $0 \leq \nu_i < p$ form a basis of the extension

$$K(t_i \mid i \in I) \,|\, K(t_i^p \mid i \in I) \; .$$

This is seen as follows. Since the elements $1, t_j, t_j^2, \ldots, t_j^{p-1}$ form a basis of the extension $K(t_i^p \mid i \in I)(t_j)|K(t_i^p \mid i \in I)$ for every $j \in I$, the products $\prod_{i \in I} t_i^{\nu_i}$ generate the above extension. If they would not be $K(t_i^p \mid i \in I)$-linearly disjoint, then there would be a non-trivial $K(t_i^p \mid i \in I)$-linear combination of them which equates to zero. Multiply by the common denominator of the coefficients. Note that in this denominator, every appearing t_i will appear to the p^m-th power for some integer $m > 0$. This yields that the result of the multiplication is a *non-trivial* K-linear combination of distinct finite products $\prod_{i \in I} t_i^{\mu_i}$ with $\mu_i \geq 0$, which equates to zero. But this contradicts our hypothesis that the t_i be K-algebraically independent. This contradiction establishes our assertion. If I has n elements, then $[K(t_i \mid i \in I) : K(t_i^p \mid i \in I)] = p^n$, and if I is infinite, then this degree is p^∞.

As we have noted already, $K(t_i \mid i \in I)^p = K^p(t_i^p \mid i \in I)$. We find that $[K(t_i \mid i \in I) : K(t_i \mid i \in I)^p] = [K(t_i \mid i \in I) : K(t_i^p \mid i \in I)] \cdot [K(t_i^p \mid i \in I) : K^p(t_i^p \mid i \in I)]$. Since the elements t_i^p are K-algebraically independent, Lemma 24.17 shows that $K^p(t_i^p \mid i \in I)$ and K are K^p-linearly disjoint. Hence, $[K(t_i^p \mid i \in I) : K^p(t_i^p \mid i \in I)]$ is equal to $[K : K^p]$, the p-degree of K. We thus find that the p-degree of a rational function field $K(t_1, \ldots, t_n)$ is equal to $[K : K^p] \cdot p^n$, and that the p-degree of $K(t_i \mid i \in I)$ is p^∞ if I is infinite. By virtue of Lemma 24.32 it follows that the p-degree of an algebraic function field $F|K$ in n variables is $[K : K^p] \cdot p^n$.

If K is perfect, then the finite products $\prod_{i \in I} t_i^{\nu_i}$, $0 \leq \nu_i < p$, form a p-basis of the rational function field $K(t_i \mid i \in I)$. For example, $1, t, \ldots, t^{p-1}$ is a p-basis of $\mathbb{F}_p(t)$ if t is transcendental over $\mathbb{F}_p$. If a field L has this p-basis, then we can write

$$L = L^p \oplus tL^p \oplus \ldots \oplus t^{p-1}L^p$$

(as an L^p-vector space).

Let again $L|K$ be an arbitrary algebraic extension and $b \in L$ with minimal polynomial f over K. Let m and $h \in K[X]$ be as in Lemma 24.26, such that $f(X) = h(X^{p^m})$ and that h is irreducible and separable over K. Then $K(b^{p^m})|K$ is a separable subextension of $L|K$, and thus lies in $(L|K)^{\rm sep}$. On the other hand, $K(b)|K(b^{p^m})$ is purely inseparable. Consequently, $L|(L|K)^{\rm sep}$ *is a purely inseparable extension.* With the help of this fact, we can deduce a lemma which is very similar to Lemma 24.14:

Lemma 24.34 *Let $L|K$ a normal and $F|K$ an arbitrary separable-algebraic field extension. Then L and F are K-linearly disjoint if and only if $L \cap F = K$. More precisely, L and F are $(L \cap F)$-linearly disjoint.*

Proof: Set $L_s := (L|K)^s$. Then $L_s|K$ is a Galois extension. Hence by Lemma 24.14, L_s and F are $(L_s \cap F)$-linearly disjoint. Since $F|K$ is separable, the same holds for $F.L_s|L_s$. Since $L|L_s$ is purely inseparable, it follows from Lemma 24.30 that L and $F.L_s$ are L_s-linearly disjoint. Hence by Lemma 24.12, L and F are $(L_s \cap F)$-linearly disjoint. Finally, observe that $L_s \cap F = L \cap F$. Indeed, since $F|K$ is separable, also $L \cap F \,|\, K$ is separable, which shows that $L \cap F$ is contained in L_s. □

We have already defined the **separable degree** $[L : K]_{\rm sep}$ **of** $L|K$ to be the number of distinct embeddings of L in $\tilde{K}$ over K. But every embedding of $(L|K)^{\rm sep}$ has a unique extension to an embedding of L since $L|(L|K)^{\rm sep}$ is purely inseparable. On the other hand, $(L|K)^{\rm sep}|K$ is separable by definition. Hence, we have that $[L : K]_{\rm sep} = [(L|K)^{\rm sep} : K]_{\rm sep} = [(L|K)^{\rm sep} : K]$. Analogously, we define the **inseparable degree of** $L|K$ to be $[L : K]_{\rm ins} := [L : (L|K)^{\rm sep}]$. By virtue of Lemma 24.27, $[L : K]_{\rm ins}$ is a power of the characteristic exponent of K. If infinite, these degrees are to be understood as supernatural numbers. We have that

$$[L : K] = [L : K]_{\rm sep} \cdot [L : K]_{\rm ins} .$$

Assume $E|K$ to be a subextension of $L|K$. Then $E.(L|K)^{\rm sep}|E$ is separable, showing that $(L|E)^{\rm sep}$ contains $E.(L|K)^{\rm sep}$. On the other hand, L is a purely inseparable extension of $E.(L|K)^{\rm sep}$ since it is already a purely inseparable extension of $(L|K)^{\rm sep}$. This shows that

$$(L|E)^{\rm sep} = E.(L|K)^{\rm sep} .$$

Applying this with $L = \tilde{K}$, we find that for every algebraic extension $E|K$,

$$E^{\rm sep} = E.K^{\rm sep} .$$

Lemma 24.35 *Let $L|K$ be an algebraic extension and $E|K$ a subextension of $L|K$. Then*

$$\begin{aligned} [L : K]_{\rm sep} &= [L : E]_{\rm sep} \cdot [E : K]_{\rm sep} , \\ [L : K]_{\rm ins} &= [L : E]_{\rm ins} \cdot [E : K]_{\rm ins} . \end{aligned}$$

Proof: We abbreviate $K' := (E|K)^{\rm sep}$ and $E' := (L|E)^{\rm sep}$. Set $L' := (L|K')^{\rm sep}$. Observe that $L' = (L|K)^{\rm sep}$ and that $E' = E.L'$. Since $E|K'$ is purely inseparable, it is linearly disjoint from $L'|K'$. Hence, $[L : K]_{\rm sep} = [L' : K] = [L' : K'][K' : K] = [E' : E][K' : K] = [L : E]_{\rm sep}[E : K]_{\rm sep}$, and $[L : K]_{\rm ins} = [L : L'] = [L : E'][E' : L'] = [L : E'][E : K'] = [L : E]_{\rm ins}[E : K]_{\rm ins}$. □

In the following, let $L|K$ be a normal extension. Let $b \in L$ and f its minimal polynomial over K. By Lemma 24.26, we choose m and $g \in K^{1/p^m}[X]$ such that $f = g^{p^m}$ and that g is irreducible and separable over K^{1/p^m}. All roots of g are roots of f. Since $L|K$ was assumed to be normal, all of them lie in L and consequently, all coefficients of g lie in $L \cap K^{1/p^\infty} = (L|K)^{\rm ins}$. This proves that b is separable over $(L|K)^{\rm ins}$. Consequently, *if $L|K$ is a normal extension, then $L|(L|K)^{\rm ins}$ is separable.* Consequently, also the extension $L\,|\,(L|K)^{\rm sep}.(L|K)^{\rm ins}$ is separable. On the other hand, $L\,|\,(L|K)^{\rm sep}$ and thus also $L\,|\,(L|K)^{\rm sep}.(L|K)^{\rm ins}$ is purely inseparable. This shows that $L\,|\,(L|K)^{\rm sep}.(L|K)^{\rm ins}$ must be trivial. We have proved that

$$\begin{aligned} L|K \text{ normal} &\implies L\,|\,(L|K)^{\rm ins} \text{ separable} \\ L\,|\,(L|K)^{\rm ins} \text{ separable} &\implies L = (L|K)^{\rm sep}.(L|K)^{\rm ins} \ . \end{aligned}$$

Lemma 24.36 *Let $L|K$ be an algebraic extension. Assume that $L\,|\,(L|K)^{\rm ins}$ is separable (which is the case if $L|K$ is normal). Then $[L : (L|K)^{\rm ins}] = [L : K]_{\rm sep}$ and $[(L|K)^{\rm ins} : K] = [L : K]_{\rm ins}$.*

Proof: Since $L\,|\,(L|K)^{\rm ins}$ is assumed to be separable, we have that $L = (L|K)^{\rm sep}.(L|K)^{\rm ins}$. The purely inseparable extension $(L|K)^{\rm ins}\,|\,K$ is linearly disjoint from the separable algebraic extension $(L|K)^{\rm sep}\,|\,K$. Hence, we find that $[L : K]_{\rm ins} = [L : (L|K)^{\rm sep}] = [(L|K)^{\rm sep}.(L|K)^{\rm ins} : (L|K)^{\rm sep}] = [(L|K)^{\rm ins} : K]$, and $[L : K]_{\rm sep} = [(L|K)^{\rm sep} : K] = [(L|K)^{\rm sep}.(L|K)^{\rm ins} : (L|K)^{\rm ins}] = [L : (L|K)^{\rm ins}]$. □

Assume $E|K$ to be a subextension of $L|K$. Then $E.(L|K)^{\rm ins}|E$ is purely inseparable, showing that $(L|E)^{\rm ins}$ contains $E.(L|K)^{\rm ins}$. On the other hand, L is a separable extension of $E.(L|K)^{\rm ins}$ since it is already a separable extension of $(L|K)^{\rm ins}$. This shows that

$$(L|E)^{\rm ins} = E.(L|K)^{\rm ins} \ .$$

Applying this with $L = \tilde{K}$, we find that for every algebraic extension $E|K$,

$$E^{1/p^\infty} = E.K^{1/p^\infty} \ .$$

Lemma 24.37 *Let $K'|K$ be an arbitrary algebraic extension and $L'|K'$ a finite extension.*
a) There is a finite extension $L|K$ such that $L' = L.K'$. If $L'|K'$ is separable, then also $L|K$ can be chosen to be separable, and if in addition $K'|K$ is purely inseparable, then $[L : K] = [L' : K']$.
b) If $L'|K'$ is purely inseparable, then there is a finite purely inseparable extension $E|K$ such that $L' \subset E.K'$.

Proof: a): We write $L' = K'(b_1, \ldots, b_n)$. Since $K'|K$ is algebraic, all b_i are algebraic over K and thus, $L := K(b_1, \ldots, b_n)$ is a finite extension which satisfies $L' = L.K'$. Now assume that $L'|K'$ is separable. Let $K_s := (K'|K)^{\rm sep}$ and $L_s := (L'|K_s)^{\rm sep}$. Then $(L'|K_s)^{\rm ins} = K'$ because $L'|K'$ is separable. For the same reason, we know that $L' = L_s.(L'|K_s)^{\rm ins} = L_s.K'$. Now we replace L' by L_s and K' by K_s in the above argument. Then every b_i is separable algebraic over K_s and hence also over K. Consequently, L will be a finite separable extension of K which satisfies $L.K' = L.K_s.K' = L_s.K' = L'$. If in addition $K'|K$ is

purely inseparable, then by Lemma 24.30, $L|K$ is linearly disjoint from $K'|K$ and thus, $[L : K] = [L.K' : K'] = [L' : K']$.

b): Let again $L' = K'(b_1, \ldots, b_n)$. If $L'|K'$ is purely inseparable, then by Lemma 24.27, L' is contained in $K'^{1/p^\infty} = K'.K^{1/p^\infty}$. To write $b_1, \ldots, b_n$ as elements of the latter product, we need finitely many elements $c_1, \ldots, c_m \in K^{1/p^\infty}$. Then $E := K(c_1, \ldots, c_m)$ is a finite purely inseparable extension of K which satisfies $L' = K'(b_1, \ldots, b_n) \subset E.K'$. □

Let $L|K$ be a normal extension. The fixed field of $\mathrm{Gal}\, L|K$ contains $(L|K)^{\mathrm{ins}}$, and we may thus identify $\mathrm{Gal}\, L|K$ with $\mathrm{Gal}\, L|(L|K)^{\mathrm{ins}}$. On the other hand, $L|(L|K)^{\mathrm{ins}}$ is separable, and Theorem 24.10 shows that the fixed field of $\mathrm{Gal}\, L|(L|K)^{\mathrm{ins}}$ is $(L|K)^{\mathrm{ins}}$. It follows that for every subextension $E|K$ of $L|K$, the fixed field of $\mathrm{Gal}\, L|E$ is $(L|E)^{\mathrm{ins}} = E.\,(L|K)^{\mathrm{ins}}$. From Theorem 24.10, we thus obtain

Theorem 24.38 *Let $L|K$ be a normal extension. The map $E \mapsto \mathrm{Gal}\, L|E$ is a bijection from the set of all subfields of L containing $(L|K)^{\mathrm{ins}}$ onto the set of all closed subgroups of $\mathrm{Gal}\, L|K$. Its inverse is the map $G \mapsto \mathrm{Fix}\,(L, G)$. For this correspondence, the rules (Gal1) – (Gal9) hold, for E, F subfields of L containing $(L|K)^{\mathrm{ins}}$, G, H closed subgroups of $\mathrm{Gal}\, L|K$ and $\sigma \in \mathrm{Gal}\, L|K = \mathrm{Gal}\, L|(L|K)^{\mathrm{ins}}$.*

If E, F are two subfields of L and if E contains $(L|K)^{\mathrm{ins}}$, then also $E.F$ contains $(L|K)^{\mathrm{ins}}$, and $E.F = E.(L|K)^{\mathrm{ins}}.F = (L|E)^{\mathrm{ins}}.\,(L|F)^{\mathrm{ins}}$. By virtue of (Gal2′), in the context of the foregoing theorem, we thus obtain the following version of (Gal2′):

Lemma 24.39 *Let $L|K$ be a normal extension with subextensions $E|K$ and $F|K$. If E is the fixed field of $\mathrm{Gal}\, L|E$ (or equivalently, if $L|E$ is separable), then $E.F$ is the fixed field of $\mathrm{Gal}\, L|E \cap \mathrm{Gal}\, L|F$.*

Lemma 24.30 gives rise to the following more general definition: An arbitrary extension $L|K$ is called **separable** if it is linearly disjoint from $K^{1/p^\infty}|K$. Hence, *if K is perfect, then every extension of K is separable.* If $L|K$ is even linearly disjoint from $\tilde{K}|K$, then $L|K$ is called **regular**. So *regularity implies separability.* Note that in these definitions, we may use a very natural amalgamation: K^{1/p^∞} and $\tilde{K}$ may both be chosen as subfields of $\tilde{L}$; it is left to the reader to show that the definition does actually not depend on the choice of the amalgamation. If $L|K$ is separable (resp. regular), then so is every subextension of $L|K$. A basic example for regular extensions is given by the following lemma, which follows directly from Lemma 24.17 and the definition of regularity:

Lemma 24.40 *If the elements x_i, $i \in I$, are K-algebraically independent, then the extension $K(x_i \mid i \in I)|K$ is regular.*

Lemma 24.41 *$L|K$ is separable if and only if it is linearly disjoint from $K^{1/p}|K$, and this is the case if and only if L^p is linearly disjoint from $K|K^p$. If $L|K$ is not separable, then there is some finite subextension $E|K$ of $K^{1/p}|K$ (which may be chosen to be linearly disjoint from $L|K$) such that E admits a non-trivial purely inseparable algebraic extension in $L.E$.*

Proof: If $L|K$ is separable, then by definition it is linearly disjoint from $K^{1/p^\infty}|K$ and thus also from $K^{1/p}|K$. For the converse, assume that $L|K$ is not linearly disjoint from $K^{1/p^\infty}|K$. Then there are K-linearly independent elements $x_1, \ldots, x_n \in L$ which are not K^{1/p^∞}-linearly independent. Choose m minimal such that there are $y_1, \ldots, y_n \in K^{1/p^m}$ with $\sum_i x_i y_i = 0$. Then $m \geq 1$, and $x_1^{p^{m-1}}, \ldots, x_n^{p^{m-1}}$ are K-linearly independent. (Otherwise, we would have a non-trivial relation $\sum_i x_i^{p^{m-1}} z_i = 0$ with $z_i \in K$, hence $\sum_i x_i z_i^{1/p^{m-1}} = 0$, contradicting the minimality of m.) But $x_1^{p^{m-1}}, \ldots, x_n^{p^{m-1}}$ are not $K^{1/p}$-linearly independent since $\sum_i x_i^{p^{m-1}} y_i^{p^{m-1}} = 0$ with $y_i^{p^{m-1}} \in K^{1/p}$. This proves that $L|K$ is not linearly disjoint from $K^{1/p}|K$.

The Frobenius is an isomorphism from $L^{1/p}$ onto L and sends the subfield L onto L^p, the subfield $K^{1/p}$ onto K and the subfield K onto $K^{1/p}$. This shows that L is linearly disjoint from $K^{1/p}|K$ if and only if L^p is linearly disjoint from $K|K^p$.

Now assume that $L|K$ is not separable, that is, not linearly disjoint from $K^{1/p}|K$. Then there exists a finite subextension $E'|K$ of $K^{1/p}|K$ which is not linearly disjoint from $L|K$. Since $E'|K$ is a finite purely inseparable extension, there are intermediate fields $K = E_0 \subset E_1 \subset \ldots \subset E_r = E'$ such that every $E_{i+1}|E_i$ is purely inseparable of degree p. Let $i \geq 0$ be the maximal index such that E_i and L are K-linearly disjoint. Then $i < r$, and it follows that E_{i+1} and $L.E_i$ are not E_i-linearly disjoint. But this means that $E_{i+1} \subset L.E_i$ because $E_{i+1}|E_i$ is of degree p. Setting $E := E_i$, we obtain that $E|K$ is linearly disjoint from $L|K$ and admits a purely inseparable extension of degree p in $L.E$. □

The p-degree does not drop under separable extensions:

Corollary 24.42 *Let K be a field of characteristic $p > 0$ and $L|K$ a separable extension. Then $[L : L^p] \geq [K : K^p]$.*

Proof: Since $L|K$ is assumed to be separable, it is linearly disjoint from $K^{1/p}|K$. Hence, $[L.K^{1/p} : L] = [K^{1/p} : K]$. Since $L^{1/p}$ contains $K^{1/p}$, we obtain that $[L^{1/p} : L] \geq [L.K^{1/p} : L] = [K^{1/p} : K]$. □

By virtue of Lemma 24.12, where we set $F = K^{1/p^\infty}$ resp. $F = \tilde{K}$, we obtain:

Lemma 24.43 *If $L|K'$ and $K'|K$ are separable resp. regular extensions, then $L|K$ is separable resp. regular.*

The converse is not true: If x is transcendental over K and $\operatorname{char} K = p > 0$, then $K(x)|K$ and $K(x^p)|K$ are regular, but $K(x)|K(x^p)$ is not separable.

Let $L|K$ be an arbitrary field extension. If it admits a transcendence basis $\mathcal{T}$ such that $L|K(\mathcal{T})$ is a separable-algebraic extension, then we say that $L|K$ is **separably generated**, and $\mathcal{T}$ is called a **separating transcendence basis**. If $L|K$ is separably generated, then it is separable; this follows from Lemma 24.40 and Lemma 24.43. For finitely generated extensions, the converse is also true:

Lemma 24.44 *If $L|K$ is a finitely generated separable extension, then a separating transcendence basis can be selected from every given set of generators.*

Proof: Let $x_1, \ldots, x_n$ be generators for L over K. Without loss of generality, we may assume that $x_1, \ldots, x_m$ are K-algebraically independent, and that $x_{m+1}, \ldots, x_n$ are algebraic

over $K(x_1, \ldots, x_m)$. If $m = n$, there is nothing to prove. Otherwise, let $f(X_1, \ldots, X_{m+1})$ be a polynomial of lowest degree with coefficients in K such that $f(x_1, \ldots, x_{m+1}) = 0$. Then f is irreducible. Assume we could write $f(X_1, \ldots, X_{m+1}) = g(X_1, \ldots, X_{m+1})^p$ where g has coefficients in $K^{1/p}$. Then $g(x_1, \ldots, x_{m+1}) = 0$ which shows that the set of monomials in $x_1, \ldots, x_{m+1}$ of degree $\leq \deg g$ is $K^{1/p}$-linearly dependent. Since $L|K$ is assumed to be separable and thus, to be linearly disjoint from $K^{1/p}|K$, it follows that this set of monomials is already K-linearly dependent. But this means that there exists a polynomial $f_1(X_1, \ldots, X_{m+1})$ of degree $\leq \deg g < \deg f$ with coefficients in K such that $f(x_1, \ldots, x_{m+1}) = 0$, a contradiction to the minimality of f. Thus, we may assume without loss of generality that X_1 does not appear in every monomial of f to a power which is divisible by p. In view of the irreducibility of f, this yields that $f(X_1, x_2, \ldots, x_{m+1})$ is a separable minimal polynomial for x_1 over $K(x_2, \ldots, x_{m+1})$. Hence, $K(x_1, \ldots, x_{m+1})$ is separable over $K(x_2, \ldots, x_{m+1})$ and thus also over $K(x_2, \ldots, x_n)$. If $x_2, \ldots, x_n$ do not already form a transcendence basis, then we iterate our procedure until we have found a separating transcendence basis among these elements. □

Lemma 24.45 *Let $L|K$ be an arbitrary extension with K relatively algebraically closed in L. Let L and F be K-algebraically disjoint in a common extension field Ω. The relative algebraic closure of F in $L.F$ is always a purely inseparable (possibly trivial) extension of F. If $F|K$ is separable, then $L|K$ and $F|K$ are linearly disjoint, and F is relatively algebraically closed in $L.F$.*

Proof: Let $\mathcal{T}$ be a transcendence basis of $F|K$. Since K is assumed to be relatively algebraically closed in L, Lemma 24.19 shows that $K(\mathcal{T})$ is relatively algebraically closed in $L(\mathcal{T})$. To prove our first assertion, we may thus assume that $F|K$ is algebraic. Abbreviate $E = (F|K)^{\text{sep}}$. Since K is relatively algebraically closed in L, we infer from Lemma 24.13 that L and K^{sep} are K-linearly disjoint. By Lemma 24.12 it follows that $L.E$ and $E^{\text{sep}} = K^{\text{sep}}$ are E-linearly disjoint. Since F is a purely inseparable extension of E, also the extension $L.F|L.E$ is purely inseparable and thus linearly disjoint from the separable extension $L.E^{\text{sep}}|L.E$. Again by Lemma 24.12, we find that $E^{\text{sep}}|E$ is linearly disjoint from $L.F|E$. Applying the same lemma a third time, we conclude that $L.F$ and $F.E^{\text{sep}} = F^{\text{sep}}$ are F-linearly disjoint and thus, $L.F \cap F^{\text{sep}} = F$. That is, the relative algebraic closure of F in $L.F$ is a purely inseparable extension of F.

To prove the second assertion, assume that $F|K$ is separable. It suffices to show for every finitely generated subextension $E|K$ of $F|K$ that $L|K$ is linearly disjoint from $E|K$ and that E is relatively algebraically closed in $L.E$. By Lemma 24.44, $E|K$ admits a separating transcendence basis $\mathcal{T}'$. Since $F|K$ is assumed to be algebraically disjoint from $L|K$, we know that the elements of $\mathcal{T}'$ are also L-algebraically independent. By Lemma 24.17, $L|K$ is linearly disjoint from $K(\mathcal{T}')|K$, and by Lemma 24.19, $K(\mathcal{T}')$ is relatively algebraically closed in $L(\mathcal{T}')$. It follows from Lemma 24.13 that $L(\mathcal{T}')|K(\mathcal{T}')$ is linearly disjoint from the separable algebraic extension $E|K(\mathcal{T}')$. By Lemma 24.12, $L|K$ is linearly disjoint from $E|K$, and by Lemma 24.13, E is relatively algebraically closed in $L.E = L(\mathcal{T}).E$. □

Lemma 24.46 *Let $L|K$ be a separable extension and $F|K$ an arbitrary extension which is algebraically disjoint from $L|K$ in a common extension field Ω. Then $L.F|F$ is a separable*

extension. If in addition, K is relatively algebraically closed in L, then F is relatively algebraically closed in $L.F$.

Proof: It suffices to prove the assertions under the assumption that $L|K$ be finitely generated. Then by Lemma 24.44, there exists a separating transcendence basis $\mathcal{T}$ of $L|K$. Since $F|K$ is algebraically disjoint from $L|K$, we know that $\mathcal{T}$ is also a transcendence basis of $L.F|F$. Since $L|K(\mathcal{T})$ is separable algebraic, the same holds for $L.F|F(\mathcal{T})$, proving that $L.F|F$ is separably generated and thus separable.

Assume in addition that K is relatively algebraically closed in L. Then by the foregoing lemma, the relative algebraic closure of F in $L.F$ is purely inseparable. But we have just proved that $L.F|F$ is separable. Hence, F is relatively algebraically closed in $L.F$. □

With the help of Lemma 24.43, we derive from the foregoing lemma:

Corollary 24.47 *If $L|K$ and $F|K$ are separable and algebraically disjoint in a common extension field Ω, then $L.F|K$ is separable. In particular, if $L|K$ is separable algebraic and $F|K$ is an arbitrary separable extension, then $L.F|K$ is separable.*

Let us have a closer look at regular extensions. A characterization of regularity reads as follows:

Lemma 24.48 *An extension $L|K$ is regular if and only if it is separable and K is relatively algebraically closed in L. If $L|K$ is not regular, then there exists a finite subextension $E|K$ of $K^{1/p}|K$ (which may be chosen to be linearly disjoint from $L|K$) such that E is not relatively algebraically closed in $L.E$.*

Proof: We have already remarked that regularity implies separability. Also, $L|K$ can not be regular if K is not relatively algebraically closed in L. Now assume that $L|K$ is separable and K is relatively algebraically closed in L. By Lemma 24.46, $L.K^{\rm sep}|K^{\rm sep}$ is separable. It is thus linearly disjoint from the purely inseparable extension $\tilde{K}|K^{\rm sep}$. On the other hand, we know from Lemma 24.13 that $L|K$ is linearly disjoint from $K^{\rm sep}|K$. Hence by Lemma 24.12, $L|K$ is linearly disjoint from $\tilde{K}|K$.

Now assume that $L|K$ is not regular. If K is not relatively algebraically closed in L, then we are done. Otherwise, $L|K$ is not separable (by what we have just proved), and our assertion follows from Lemma 24.41. □

Lemma 24.49 *Let $F|K$ be a regular extension and $L|K$ an arbitrary extension which is algebraically disjoint from $F|K$ in a common extension field Ω. Then $L|K$ is linearly disjoint from $F|K$, and $F.L|L$ is regular.*

Proof: By definition, $F|K$ is linearly disjoint from $\tilde{K}|K$. Hence by Lemma 24.12, $F.K'|K'$ is linearly disjoint from $\tilde{K}'|K'$ for every algebraic extension $K'|K$. That is, $F.K'|K'$ is regular. We take K' to be the relative algebraic closure of K in L. Since $F.K'|K'$ is separable by the foregoing lemma and since K' is relatively algebraically closed in L, we can infer from Lemma 24.46 that $F.K'|K'$ is linearly disjoint from $L|K'$. Since also $K'|K$ is linearly disjoint from $F|K$, we can deduce from Lemma 24.12 that $L|K$ is linearly disjoint from $F|K$.

The whole argument works equally well if we replace L by $\tilde{L}$. Indeed, if $L|K$ is algebraically disjoint from $F|K$, then so is $\tilde{L}|K$ since every transcendence basis of $L|K$ is a transcendence basis of $\tilde{L}|K$. We obtain that $F|K$ is linearly disjoint from $\tilde{L}|K$. By virtue of Lemma 24.12, this shows that $F.L|L$ is linearly disjoint from $\tilde{L}|L$, that is, $F.L|L$ is regular. □

With the help of Lemma 24.43, we derive from the foregoing lemma:

Corollary 24.50 *If $L|K$ and $F|K$ are regular and algebraically disjoint in a common extension field Ω, then $L.F|K$ is regular.*

From the above lemma, we can also deduce the following analogue to Lemma 24.19:

Corollary 24.51 *Let $F|K$ be a regular extension and $\mathcal{T}$ a set of elements which are F-algebraically independent (in some field extension of F). Then $F(\mathcal{T})|K(\mathcal{T})$ is regular.*

For the conclusion of this section, let note that there exist inseparable extensions $L|K$ where K is relatively algebraically closed in L:

Example 24.52 Let t, x, y be algebraically independent over $\mathbb{F}_p$ and set $L := \mathbb{F}_p(t, x, y)$. Define

$$s := x^p + ty^p \quad \text{and} \quad K := \mathbb{F}_p(t, s)\ .$$

Then K is relatively algebraically closed in L. To show this, let $b \in L$ be algebraic over K. Note that x is transcendental over K. Indeed, otherwise x and thus also y would be algebraic over K, so that $\operatorname{trdeg} L|\mathbb{F}_p = \operatorname{trdeg} K|\mathbb{F}_p \leq 2$ in contradiction to our assumption that t, x, y be algebraically independent over $\mathbb{F}_p$. The element b^p is algebraic over K and lies in $L^p = \mathbb{F}_p(t^p, x^p, y^p)$ and thus also in $K(x) = \mathbb{F}_p(t, x, y^p)$. Since x is transcendental over K, it follows by Lemma 24.17 that $b^p \in K$. Consequently, $b \in K^{1/p}$. Since $\mathbb{F}_p$ is perfect, we have that $K^{1/p} = \mathbb{F}_p(t^{1/p}, s^{1/p})$. Write

$$b \ = \ r_0 + r_1 s^{\frac{1}{p}} + \ldots + r_{p-1} s^{\frac{p-1}{p}} \qquad \text{with} \ \ r_i \in \mathbb{F}_p(t^{1/p}, s) = K(t^{1/p})\ .$$

By the definition of s,

$$b \ = \ r_0 \ + \ r_1 x + \ldots + r_{p-1} x^{p-1} \ + \ldots + \ t^{1/p} r_1 y + \ldots + t^{(p-1)/p} r_{p-1} y^{p-1}$$

(in the middle, we have omitted the summands in which both x and y appear). Since x, y are algebraically independent over $\mathbb{F}_p$, the degree of inseparability of K is p^2, and the elements $x^i y^j$, $0 \leq i < p$, $0 \leq j < p$, form a basis of $\mathbb{F}_p(x, y)|\mathbb{F}_p(x^p, y^p)$. Since t and $t^{1/p}$ are transcendental over $\mathbb{F}_p(x^p, y^p)$, we know that $\mathbb{F}_p(x, y)|\mathbb{F}_p(x^p, y^p)$ is linearly disjoint from $\mathbb{F}_p(t, x^p, y^p)|\mathbb{F}_p(x^p, y^p)$ and from $\mathbb{F}_p(t^{1/p}, x^p, y^p)|\mathbb{F}_p(x^p, y^p)$. This shows that the elements $x^i y^j$, $0 \leq i < p$, $0 \leq j < p$, form a basis of $L|\mathbb{F}_p(t, x^p, y^p)$ and are still $\mathbb{F}_p(t^{1/p}, x^p, y^p)$-linearly independent. Hence, b can also be written as a linear combination of these elements with coefficients in $\mathbb{F}_p(t, x^p, y^p)$, and this must coincide with the above $\mathbb{F}_p(t^{1/p}, x^p, y^p)$-linear combination which represents b. That is, all coefficients r_i *and* $t^{i/p} r_i$, $1 \leq i < p$, are in $\mathbb{F}_p(t, x^p, y^p)$. This is impossible unless they are zero. It follows that $b = r_0 \in K(t^{1/p})$. Assume that $b \notin K$. Then $[K(b) : K] = p$ and thus, $K(b) = K(t^{1/p})$ since also $[K(t^{1/p}) : K] = p$. But then $t^{1/p} \in K(b) \subset L$, a contradiction. This proves that K is relatively algebraically closed in L.

On the other hand, $t^{1/p} = y^{-1}(s^{1/p} - x) \in L(s^{1/p})$. Hence, $L.K^{1/p} = L(t^{1/p}, s^{1/p}) = L(s^{1/p})$ and

$$[L.K^{1/p} : L] \;=\; [L(s^{1/p}) : L] \;\leq\; p < p^2 \;=\; [K^{1/p} : K]\,.$$

That is, $L|K$ is not linearly disjoint from $K^{1/p}|K$ and thus not separable. Although being finitely generated, $L|K$ is consequently not separably generated; in particular, it is not a rational function field. At the same time, we have seen that $K(s^{1/p})$ admits a non-trivial purely inseparable algebraic extension in $L(s^{1/p})$ (namely, $K^{1/p}$). On the other hand, $K(s^{1/p})$ and L are K-linearly disjoint because $s^{1/p} \notin L$. In particular,

$$[L.K^{1/p} : L] \;=\; [L(s^{1/p}) : L] \;=\; p\,.$$

Let us also observe that in the last statements, s can be replaced by any other element a of K which does not lie in K^p. Indeed, we know that $a^{1/p} \notin L$ since K is relatively algebraically closed in L. Hence, $K(s^{1/p})$ and L are K-linearly and $[L(a^{1/p}) : L] = p = [L.K^{1/p} : L]$. This shows that $L(a^{1/p}) = L.K^{1/p}$ and that $K(a^{1/p})$ admits the non-trivial purely inseparable algebraic extension $K^{1/p}$ in $L(a^{1/p})$.

Let us prove even more: if $K_1|K$ is any proper inseparable algebraic extension, then $t^{1/p} \in L.K_1$. Take such an extension $K_1|K$. Then there is some separable-algebraic subextension $K_2|K$ and an element $a \in K_1 \setminus K_2$ such that $a^p \in K_2$. Since $K_2|K$ is separable and K is relatively algebraically closed in L, we see that K_2 is relatively algebraically closed in $L_2 := L.K_2$. Hence, $a \notin L_2$ and therefore, $[L_2(a) : L_2] = p$. On the other hand, $K_2^{1/p} = K^{1/p}.K_2$ and thus, $L_2.K_2^{1/p} = L_2.K^{1/p} = L.K^{1/p}.K_2$. Consequently, $[L.K^{1/p} : L] = p$ implies that $[L_2.K_2^{1/p} : L_2] = [L.K^{1/p}.K_2 : L.K_2] \leq p$. Since $a \in K_2^{1/p} \subset L_2.K_2^{1/p}$ and $[L_2(a) : L_2] = p$, it follows that $L_2.K_2^{1/p} = L_2(a)$. We obtain:

$$t^{1/p} \in K^{1/p} \;\subseteq\; K_2^{1/p} \;\subseteq\; L_2.K_2^{1/p} \;=\; L_2(a) \;\subseteq\; L.K_1\,.$$

Finally, let us observe that the relative algebraic closure F of K in $\mathbb{F}_p((t))$ since otherwise $t^{1/p} \in L.F$, which contradicts the fact that $L.F \subseteq \mathbb{F}_p((t))$. From Lemma 24.32 it follows that the degree of inseparability of F is p^2 like that of K. ♢

Exercise 24.4 *Let $L|K$ be separable. Given K-linearly independent elements $x_1, \ldots, x_n \in L$, prove that also $x_1^{p^\mu}, \ldots, x_n^{p^\mu}$ are K^{p^ν}-linearly independent, for every all integers μ, ν.*

Exercise 24.5 *Show that if k is relatively separable-algebraically closed in K, then k^{1/p^∞} is relatively algebraically closed in K^{1/p^∞}. (Hint: Otherwise, $K^{1/p^\infty}|k$ would admit a proper separable algebraic subextension. But this is linearly disjoint from $K|k$ and thus also from $K^{1/p^\infty}|k$, contradiction.) Is the converse also true?*

24.8 (Pro-) p-groups and p'-groups

Let p be a prime. A (not necessarily finite) torsion group in which the orders of all elements are a power of p is called a **p-group**. For example, an abelian torsion group A is a p-group if and only if $\#A$ divides p^∞. A torsion group will be called a **p'-group** (read: "*p-prime*-group") if the orders of all elements are prime to p. A profinite group is called a **pro-p-group** if it is the inverse limit of an inverse system of p-groups (or equivalently, if all of its finite quotients are p-groups), and it is called a **pro-p'-group** if it is the inverse limit of an inverse system of p'-groups. A finite pro-p-group is a p-group (and similarly

for p'). The property of being a pro-p-group (resp. a pro-p'-group) is inherited by closed subgroups and quotients by closed subgroups. A field extension is called a **p-extension** if it is Galois and its Galois group is a pro-p-group, and it is called a **p'-extension** if it is Galois and its Galois group is a pro-p'-group. A field extension is a p-extension if and only if each of its finite subextensions is a p-extension (and similarly for p').

Let us now collect some statements about p-groups.

Lemma 24.53 *If G is a finite p-group and H is a proper subgroup of G, then there exists a subgroup G_1 of G such that $H \lhd G_1$ and $(G_1 : H) = p$.*

Proof: Note that $G \neq \{1\}$ by the assumption on H. We claim that the center $C(G) = \{g \in G \mid \forall h \in G : \ hg = gh\}$ is non-trivial. Assume the contrary. Then the centralizer $C_G(h) = \{g \in G \mid hg = gh\}$ would be a proper subgroup of G for every element $h \in G \setminus \{1\}$. This would mean that 1 is the only element of G whose orbit under conjugation has a length which is not divisible by p; but this is impossible in a group whose order is a power of p (because the order of a finite group G is the sum of the lengths of the orbits in G). This contradiction proves our claim.

Assume that $C(G) \subset H$. Then by induction on the order of G, the assertion of our lemma follows for the groups $G/C(G)$ and $H/C(G)$. That is, there is a subgroup G_1 of G containing $C(G)$ such that $H/C(G) \lhd G_1/C(G)$ and $(G_1/C(G) : H/C(G)) = p$. It follows that $H \lhd G_1$ and $(G_1 : H) = p$.

Finally, assume that $C(G) \not\subset H$. Then there exists some $g \in C(G) \setminus H$ such that $g^p \in H$. Then $G_1 := \langle g \rangle H$ is the required subgroup of G since the assertions $H \lhd G_1$ and $(G_1 : H) = p$ follow from the fact that g commutes with H. □

The **Frattini subgroup** of an arbitrary finite group G is defined to be the intersection of all maximal proper subgroups of G and is denoted by $\Phi(G)$. A group G is called **elementary-abelian** if it is of the form $\mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_n\mathbb{Z}$ for (not necessarily distinct) prime numbers $p_1, \ldots, p_n$. Consequently, an elementary-abelian p-group is a finite product of copies of $\mathbb{Z}/p\mathbb{Z}$, that is, a finite dimensional $\mathbb{F}_p$-vector space.

Theorem 24.54 *Let G be any finite p-group.*
a) If H is a maximal proper subgroup of G, then $H \lhd G$ and $(G : H) = p$. Consequently, $G/\Phi(G)$ is elementary-abelian.
b) For every subgroup $H \subset G$ there exists a chain of subgroups $H = H_0 \subset H_1 \subset \ldots \subset H_n = G$ such that $H_{i-1} \lhd H_i$ and $(H_i : H_{i-1}) = p$ for $i = 1, \ldots, n$. In particular, every finite p-group is solvable.

Proof: a) Let H be a maximal proper subgroup of G. We choose G_1 according to the foregoing lemma. Then $G_1 = G$ by the maximality of H. Hence, $H \lhd G$ and $(G : H) = p$. Now let $H_1, \ldots, H_n$ be all maximal proper subgroups of G. By what we have shown, they are normal subgroups of G. Now we use the isomorphism (24.2), where N_1, N_2 are normal subgroups of G. By induction on the number of normal subgroups, we find

$$G/\Phi(G) = G/(H_1 \cap \ldots \cap H_n) \cong G/H_1 \times \ldots \times G/H_n .$$

By what we have already shown, the latter is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \ldots \times \mathbb{Z}/p\mathbb{Z}$, which is an elementary-abelian group.

b) The first assertion follows from the foregoing lemma by induction on $(G : H)$. The second assertion follows from the first by taking $H = \{1\}$. □

A profinite group is called **prosolvable** if it is the limit of an inverse system of finite solvable groups. From the foregoing theorem, we obtain the following analogue assertions for pro-p-groups.

Corollary 24.55 *Let G be any pro-p-group.*
a) If H is a maximal proper closed subgroup of G, then H is an open normal subgroup of G and $(G : H) = p$. Consequently, $G/\Phi(G)$ is an $\mathbb{F}_p$-vector space.
b) G is prosolvable. For every open subgroup $H \subset G$ there exists a chain of open subgroups $H = H_0 \subset H_1 \subset \ldots \subset H_n = G$ such that $H_{i-1} \lhd H_i$ and $(H_i : H_{i-1}) = p$ for $i = 1, \ldots, n$.

Proof: a): The closed subgroup H is contained in some proper open subgroup. Hence, if it is a maximal proper closed subgroup of G, then it is open. It contains an open normal subgroup N. By the foregoing theorem, the finite p-group G/N admits a normal subgroup of index p. Its foreimage in G is a normal subgroup of index p in G, containing H. By the maximality of H, it is equal to H.

As in the finite case, one shows that there is an epimorphism from G onto $\prod_i G/H_i$, where H_i runs through all maximal proper closed subgroups, and that its kernel is $\Phi(G)$. Since every G/H_i is isomorphic to $\mathbb{F}_p$, the product is an $\mathbb{F}_p$-vector space.

b): By the foregoing theorem, every finite p-group is solvable. So by definition, a pro-p-group is prosolvable. The second assertion is shown similarly to the first assertion of a). □

Corollary 24.56 *Every finite subextension of a p-extension of a field K is a tower of Galois extensions of degree p (which are Artin-Schreier extensions if p is the characteristic of K). Every finite subextension of an extension of degree a power of p is a tower of extensions of degree p.*

Proof: Let $L|K$ be a finite subextension of the p-extension $L_1|K$. Then L_1 contains the normal hull L_0 of L over K. Hence, $L_0|K$ is a finite p-extension. Hence, $G = \operatorname{Gal} L_0|K$ is a finite p-group. We apply part b) of Theorem 24.54 to its subgroup $H = \operatorname{Gal} L_0|L$ and set $K_i = \operatorname{Fix}(L_0, H_{n-i})$, $i = 0, \ldots, n$. Since $H_{n-i} \lhd H_{n-i+1}$ and $(H_{n-i+1} : H_{n-i}) = p$, we have that $K_i|K_{i-1}$ is a Galois extension of degree p, for every $i = 1, \ldots, n$.

We have already noted that a Galois extension of degree p of a field of characteristic p is an Artin-Schreier extension; see Corollary 12.29. □

A subgroup H of a profinite group G is called a **p-Sylow group of** G if it is a closed pro-p-subgroup of G such that p does not divide $(G : H)$. If H is a p-Sylow group of G, then for every open normal subgroup N of G we find that $H.N/N$ is a p-Sylow group of the finite group G/N. Indeed, $H.N/N$ is a p-group, and since p does not divide $(G : H)$, it does not divide $(G : H.N) = (G/N : H.N/N)$. The following is a generalization of the Sylow Theorems of finite group theory:

Theorem 24.57 *Let p be a prime and G a profinite group. Then for every pro-p-subgroup G_0 of G, there exists a p-Sylow group H of G containing G_0. All p-Sylow groups of G are conjugate.*

Proof: Let N_i, $i \in I$, be the family of all open normal subgroups of G and recall the discussion preceding to Lemma 24.8. For every $i \in I$, the subgroup $G_0.N_i/N_i$ of the finite group G/N_i is a p-group. By finite group theory, the set of p-Sylow groups of G/N_i containing $G_0.N_i/N_i$ is finite and nonempty; denote this set by $\mathcal{S}_i$. If $i, j \in I$ such that $N_j \subset N_i$, then by the Sylow Theorems of finite group theory, the canonical epimorphism $\eta_{ji} : G/N_j \to G/N_i$ maps a pro-p-group of G/N_j containing $G_0.N_j/N_j$ onto a pro-p-group of G/N_i containing $G_0.N_i/N_i$. Thus, η_{ji} induces a map $\pi^{\mathcal{S}}_{ji}$ from $\mathcal{S}_j$ into $\mathcal{S}_i$. The reader may verify that the maps $\pi^{\mathcal{S}}_{ji}$ satisfy (INV1) and (INV2). Since also I satisfies (INV0) for the partial ordering that we have introduced preceding to Lemma 24.8, Lemma 24.7 shows that the inverse limit over the sets $\mathcal{S}_i$ is nonempty. Let $(H_i)_{i\in I}$ be an element of it. Then via the isomorphism $G \cong \varprojlim G/N_i$, the profinite group $\varprojlim H_i$ is a subgroup of G. Since every H_i is a p-Sylow group containing $G_0.N_i/N_i$, it follows that H is a pro-p-group containing $G_0 \cong \varprojlim G_0.N_i/N_i$. Further, p does not divide $(G/N_i : H_i)$. But $H_i = H.N_i/N_i$ and consequently, $(G/N_i : H_i) = (G/N_i : H.N_i/N_i) = (G : H.N_i)$. Hence, p does not divide $\mathrm{lcm}_i(G : H.N_i) = (G : H)$, showing that H is a p-Sylow group of G.

Now let H and $\mathcal{H}$ be p-Sylow groups of G. Let $i, j \in I$. Then $H.N_i/N_i$ and $\mathcal{H}.N_i/N_i$ are p-Sylow groups of the finite group G/N_i. Hence by the Sylow Theorems of finite group theory, the set $\mathcal{C}_i := \{g_i \in G/N_i \mid g_i(H.N_i/N_i)g_i^{-1} = \mathcal{H}.N_i/N_i\}$ is nonempty, and it is finite. If $N_j \subset N_i$, then the canonical epimorphism η_{ji} induces a map $\pi^{\mathcal{C}}_{ji}$ from $\mathcal{C}_j$ into $\mathcal{C}_i$. The maps $\pi^{\mathcal{C}}_{ji}$ satisfy (INV1) and (INV2). Hence, Lemma 24.7 shows that the inverse limit over the sets $\mathcal{C}_i$ is nonempty. Let $g = (g_i)_{i\in I}$ be an element of it. Via the isomorphism $G \cong \varprojlim G/N_i$, it is in fact an element of G which satisfies $gHg^{-1} = \mathcal{H}$. □

If H is the unique p-Sylow group of the profinite group G, then H is a closed normal subgroup of G, and G/H is a pro-p'-group.

To conclude this section, we introduce a sort of groups which behave very much like Galois groups (and indeed, we show a connection to Galois groups in our chapter on ramification theory. Given an arbitrary abelian torsion group Γ and a field k of characteristic exponent p, then $\mathrm{Hom}(\Gamma, k^\times)$ denotes the set of all homomorphisms from Γ into the multiplicative group $k^\times$ of k. Given $\chi, \chi' \in \mathrm{Hom}(\Gamma, k^\times)$ then we define the product $\chi \cdot \chi'$ by $\chi \cdot \chi'(g) = \chi(g)\chi'(g)$ for every $g \in \Gamma$. In this way, $\mathrm{Hom}(\Gamma, k^\times)$ becomes a group, called a **p-character group of** Γ. Its elements are called **characters**. Its identity element is the **trivial character** 1 which sends every g to $1 \in k^\times$. The inverse of χ sends every g to $\chi(g)^{-1}$.

If k is algebraically closed, then $\mathrm{Hom}(\Gamma, k^\times)$ is called the **full p-character group of** Γ. Since every element of Γ has finite order by assumption, $\chi(\Gamma)$ is contained in the group of roots of unity of the field k, for every character χ. So we see that the group does actually not depend upon the field k but rather upon the group of roots of unity contained in it. So one may actually replace k by the relative algebraic closure of its prime field in k. In particular, all algebraically closed fields of a fixed characteristic p have the same group of roots of unity, and so the full character group for a given group Γ only depends upon the characteristic of k.

We leave it to the reader to show the following:

$$\Gamma = \Gamma_1 \oplus \Gamma_2 \implies \mathrm{Hom}(\Gamma, k^\times) = \mathrm{Hom}(\Gamma_1, k^\times) \oplus \mathrm{Hom}(\Gamma_2, k^\times)\ . \tag{24.4}$$

Let q be any prime or equal to 1. Every abelian torsion group Γ admits a decomposition $\Gamma = \Gamma_q \oplus \Gamma_{q'}$ where Γ_q is the subgroup of all elements of Γ whose order is a power of q, and $\Gamma_{q'}$ is the subgroup of all elements of Γ whose order is prime to q. Hence, Γ_q is an abelian q-group, and $\Gamma_{q'}$ is an abelian q'-group. We have

$$\mathrm{Hom}(\Gamma, k^\times) = \mathrm{Hom}(\Gamma_q, k^\times) \oplus \mathrm{Hom}(\Gamma_{q'}, k^\times) \ .$$

We know that over a field of characteristic exponent p, the polynomial $X^{p^n} - 1$ splits into linear factors, for every $n \in \mathbb{N}$. Hence, 1 is the only element of order a power of p in the group of roots of unity in a field k of characteristic exponent p. This yields that 1 is the only element of order a power of p in $\mathrm{Hom}(\Gamma, k^\times)$, that is, $\mathrm{Hom}(\Gamma, k^\times)$ is a p'-group and $\mathrm{Hom}(\Gamma_p, k^\times) = \{1\}$. In other words,

$$\mathrm{charexp}\, k = p \implies \mathrm{Hom}(\Gamma, k^\times) = \mathrm{Hom}(\Gamma_{p'}, k^\times) \ . \tag{24.5}$$

Lemma 24.58 *If Γ is finite and k is algebraically closed of characteristic exponent p, then* $\mathrm{Hom}(\Gamma, k^\times) \cong \Gamma_{p'}$.

Proof: By the Main Theorem on Finitely Generated Abelian Groups, we can write Γ as a finite direct sum of cyclic groups, all of them finite since Γ is finite. In view of (24.4) and (24.5), it remains to show that $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, k^\times) \cong \mathbb{Z}/m\mathbb{Z}$ for every natural number which is prime to p. But for every such m, the group $\mu_{k,m}$ of m-th roots of unity contained in the algebraically closed field k is isomorphic to $\mathbb{Z}/m\mathbb{Z}$. On the other hand, if η is a generator of $\mathbb{Z}/m\mathbb{Z}$, then for every m-th root of unity ζ, there is precisely one character $\chi \in \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, k^\times)$ such that $\chi(\eta) = \zeta$. This proves that $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, k^\times) \cong \mu_{k,m} \cong \mathbb{Z}/m\mathbb{Z}$. □

Suppose that Δ is a subgroup of the abelian torsion group Γ. We leave it to the reader to prove the following facts. If $\mathrm{Hom}(\Gamma, k^\times)$ is the full p-character group of Γ, then every character in $\mathrm{Hom}(\Delta, k^\times)$ can be extended to a character in $\mathrm{Hom}(\Gamma, k^\times)$. Consequently, the restriction map $\mathrm{Hom}(\Gamma, k^\times) \to \mathrm{Hom}(\Delta, k^\times)$ is surjective. Its kernel is the subgroup of all characters of Γ which are trivial on Δ; we will denote it by $\mathrm{Hom}_\Delta(\Gamma, k^\times)$. Note that $\mathrm{Hom}_\Delta(\Gamma, k^\times)$ is canonically isomorphic to $\mathrm{Hom}(\Gamma/\Delta, k^\times)$. Since every element of Γ is already contained in some finite subgroup, $\mathrm{Hom}(\Gamma, k^\times)$ is the inverse limit of the inverse system of the finite groups $\mathrm{Hom}(\Delta_i, k^\times)$, where Δ_i runs through all finite subgroups of Γ. Hence, $\mathrm{Hom}(\Gamma, k^\times)$ is a profinite group. The subgroups $\mathrm{Hom}_{\Delta_i}(\Gamma, k^\times)$ form a basis of the neighborhood filter of the trivial character 1 of Γ.

Exercise 24.6 *Let G be a profinite group. Prove:*
a) If $\eta : G \to G_1$ is an epimorphism of profinite groups and if H is a p-Sylow group of G, then $\eta(H)$ is a p-Sylow group of H.
b) $\#G = \prod_q \#H_q$ where q runs through all primes and every H_q is a q-Sylow group of G.
What can be said about the number of p-Sylow groups of G?

Exercise 24.7 *Describe a Galois correspondence of character groups.*

24.9 G-modules and group complements

In this section, we introduce some notions that we will need in the next section. Take any group G. For $\rho \in G$, **conjugation by** ρ means the automorphism

$$G \ni \tau \;\mapsto\; \tau^\rho \;:=\; \rho^{-1}\tau\rho \;.$$

Note that

$$\tau^{\sigma\rho} = \rho^{-1}\sigma^{-1}\tau\,\sigma\,\rho = \rho^{-1}(\tau^\sigma)\rho = (\tau^\sigma)^\rho \quad \text{for all } \tau,\sigma,\rho \in G\;. \tag{24.6}$$

Further, we set $\tau^{-\sigma} := (\tau^{-1})^\sigma$ (which indeed is the inverse of τ^σ). As usual, we set $M^\sigma = \{m^\sigma \mid m \in M\}$ for every subset $M \subset G$. A subgroup N is normal in G if and only if $N^\sigma = N$ for all $\sigma \in G$. We always have $G^\sigma = G$. Hence, if H is a group complement of the normal subgroup N in G, that is,

$$HN = G \quad \text{and} \quad H \cap N = \{1\}\;, \tag{24.7}$$

then so is every conjugate H^σ for $\sigma \in G$. Uniqueness up to conjugation would mean that these are the only group complements of N in G.

We shall now introduce two notions that play an important role in Section 12.6. A **right G-module** is an arbitrary group N together with a map μ from G into the group of automorphisms of N such that $\mu(\sigma\rho) = \mu(\rho) \circ \mu(\sigma)$. For example, to every $\sigma \in G$ we may associate the conjugation by σ; in view of (24.6), this turns G into a right G-module. In this setting, a subgroup N of G is normal if and only if it is a G-submodule of G.

Also in the general case of right G-modules N, it is convenient to use the above notation and write a^ρ instead of $\mu(\rho)(a)$ for $a \in N$. A map ϕ from G into a G-module N is called a **crossed homomorphism** if it satisfies

$$\phi(\sigma\rho) = \phi(\sigma)^\rho\phi(\rho) \quad \text{for all } \sigma,\rho \in G\;. \tag{24.8}$$

As for a usual homomorphism, also the kernel of a crossed homomorphism is a subgroup of G, but it may not be normal in G.

Let us assume that H is a group complement of the normal subgroup N in G. It follows from (24.7) that every element $\sigma \in G$ admits a unique representation

$$\sigma = \sigma_H\sigma_N \quad \text{with } \sigma_H \in H\,,\ \sigma_N \in N \tag{24.9}$$

Note that H is a system of representatives for the left cosets of G modulo N. Since $N \lhd G$, we have $HN = NH$, and H is also a system of representatives for the right cosets of G.

Now assume in addition that N is abelian. Then the scalar multiplication of the G-module N given by conjugation reads as

$$\sigma^\rho = \rho_N^{-1}(\rho_H^{-1}\sigma\rho_H)\rho_N = \rho_H^{-1}\sigma\rho_H = \sigma^{\rho_H} \quad \text{for all } \sigma \in N\,,\ \rho \in G \tag{24.10}$$

since ρ_N and $\rho_H^{-1}\sigma\rho_H$ are elements of N. According to (24.9) and (24.10) we write

$$\sigma\rho = \sigma_H\sigma_N\rho_H\rho_N = \sigma_H\rho_H\rho_H^{-1}\sigma_N\rho_H\rho_N = \sigma_H\rho_H\sigma_N^\rho\rho_N\;.$$

Hence, the projection $\sigma \mapsto \sigma_H$ onto the first factor in (24.9) is the canonical epimorphism from G onto H with kernel N. The other projection $\sigma \mapsto \sigma_N$ is a crossed homomorphism from G onto N, satisfying

$$(\sigma\rho)_N = \sigma_N^\rho \rho_N \quad \text{for all } \sigma, \rho \in G\ ; \tag{24.11}$$

it induces the identity on N, and its kernel is H.

Exercise 24.8 *Take a crossed homomorphism ϕ. Show that*
1) $\phi(1) = 1$,
2) ϕ is injective if and only if its kernel is trivial (hint: first compute $\phi(b^{-1})$ in terms of $\phi(b)$, then compute $\phi(b^{-1}a)$ under the assumption that $\phi(a) = \phi(b)$).

24.10 The Taylor expansion of a polynomial

We frequently need a Taylor expansion of polynomials which works in fields of arbitrary characteristic. For every $j \in \mathbb{N}$, we have

$$(X+Y)^j = \sum_{i=0}^{n} \left(\begin{array}{c} j \\ i \end{array} \right) X^{j-i} Y^i\ .$$

This is also true in fields of characteristic $p > 0$ since the binomial coefficients are natural numbers which then will be taken modulo p. For an arbitrary polynomial $f(X) = c_n X^n + c_{n-1} X^{n-1} + \ldots + c_0$, summation now gives

$$f(X+Y) = \sum_{j=0}^{n} \sum_{i=0}^{j} c_j \left(\begin{array}{c} j \\ i \end{array} \right) X^{j-i} Y^i = \sum_{i=0}^{n} \sum_{j=i}^{n} c_j \left(\begin{array}{c} j \\ i \end{array} \right) X^{j-i} Y^i\ .$$

Setting

$$f_i(X) := \sum_{j=i}^{n} c_j \left(\begin{array}{c} j \\ i \end{array} \right) X^{j-i} = \sum_{j=0}^{n-i} c_{j+i} \left(\begin{array}{c} j+i \\ i \end{array} \right) X^j \tag{24.12}$$

which we will call the **i-th derivative of f**, we obtain the **Taylor expansion**

$$f(X+Y) = \sum_{i=0}^{n} f_i(X) Y^i\ . \tag{24.13}$$

All i-th derivatives of f are defined also over fields of positive characteristic, but for certain i they may vanish identically (even if $i \leq n$). Over fields of characteristic 0, we have

$$f_i(X) = \sum_{j=i}^{n} c_j \left(\begin{array}{c} j \\ i \end{array} \right) X^{j-i} = \sum_{j=i}^{n} c_j \frac{1}{i!} \frac{d^i}{dX^i} X^j = \frac{1}{i!} f^{(i)}(X)$$

which gives the well-known Taylor identity

$$f(X+Y) = \sum_{i=0}^{n} \frac{1}{i!} f^{(i)}(X) Y^i\ .$$

The same identity can be used over fields of characteristic $p > 0$ for $n < p$; for i not prime to p, the factor $\frac{1}{i!}$ makes no sense. But in any case, we have

$$f_1(X) = f^{(1)}(X) = f'(X) \quad \text{and} \quad f_0(X) = f(X)\ .$$

Further, let us compute the j-th derivative of an i-th derivative:

$$\begin{aligned}(f_i)_j(X) &= \left(\sum_{\nu=i}^{n} c_\nu \binom{\nu}{i} X^{\nu-i}\right)_j = \sum_{\nu=i+j}^{n} c_\nu \binom{\nu}{i}\binom{\nu-i}{j} X^{\nu-i-j} \\ &= \sum_{\nu=i+j}^{n} c_\nu \frac{(i+j)!}{i!j!}\binom{\nu}{i+j} X^{\nu-(i+j)} = \frac{(i+j)!}{i!j!} f_{i+j}(X) \\ &= \binom{i+j}{i} f_{i+j}(X) = \binom{i+j}{j} f_{i+j}(X)\,.\end{aligned}$$

Setting $j = k - i$, we find

$$(f_i)_{k-i}(X) = \binom{k}{i} f_k(X)\,,$$

whence by virtue of (24.13),

$$f_i(X+Y) = \sum_{k=0}^{n-i}(f_i)_k(X)Y^k = \sum_{k=i}^{n}(f_i)_{k-i}(X)Y^{k-i} = \sum_{k=i}^{n}\binom{k}{i} f_k(X)Y^{k-i}\,.$$

Putting $Y := Z - X$, we derive the following versions of the Taylor expansion (24.13) and of the last equation:

$$f(Z) = \sum_{k=0}^{n} f_i(X)(Z-X)^i \tag{24.14}$$

$$f_i(Z) = \sum_{k=i}^{n}\binom{k}{i} f_k(X)(Z-X)^{k-i}\,. \tag{24.15}$$

From equations (24.12) and (24.14) we obtain:

Lemma 24.59 *Let R be a subring of an arbitrary field K, and let $f \in R[X]$. Then all derivatives of f lie in $R[X]$. Further, there exist $G_f(X,Z), H_f(X,Z) \in R[X,Z]$ such that*

$$f(Z) - f(X) = (Z-X)G_f(X,Z) = f'(X)(Z-X) + (Z-X)^2 H_f(X,Z)\,.$$

We also need a multidimensional version of the last assertion of the foregoing lemma. In the following, let f be a polynomial in the n variables $X_1, \ldots, X_n$, with coefficients in a subring R of an arbitrary field K. We write $\underline{X} = (X_1, \ldots, X_n)$ and $f = f(\underline{X})$. Given a second n-tuple $\underline{Y} = (Y_1, \ldots, Y_n)$ of variables, we consider the polynomial $f(\underline{X} + \underline{Y})$. It is the sum over monomials of the form

$$g(\underline{X} + \underline{Y}) = c(X_1 + Y_1)^{m_1} \cdot \ldots \cdot (X_n + Y_n)^{m_n}\,.$$

Viewing $f(\underline{X} + \underline{Y})$ and $g(\underline{X} + \underline{Y})$ as polynomials in the variables $X_1, \ldots, X_n, Y_1, \ldots, Y_n$, we ask for the monomials which are linear in one single Y_j. Evaluating $g(\underline{X} + \underline{Y})$ by means of the binomial expansion, we find just one such monomial for every j, namely

$$cX_1^{m_1} \cdot \ldots \cdot m_j X_j^{m_j - 1} Y_j \cdot \ldots \cdot X_n^{m_n}\,.$$

This is in fact equal to

$$\frac{\partial g}{\partial X_j}(\underline{X}) \cdot Y_j \ ,$$

where the first factor is the partial derivative of $g(\underline{X})$ with respect to X_j. Summing up over all monomials g in f and using the fact that the partial derivative is additive, we find that

$$\frac{\partial f}{\partial X_j}(\underline{X}) \cdot Y_j$$

is the sum of all monomials of $f(\underline{X} + \underline{Y})$ which are linear in Y_j. Similarly, one finds that the monomials which contain no Y_j at all, just sum up to $f(\underline{X})$. Consequently, there are polynomials $\hat{h}_{jk}(\underline{X}, \underline{Y})$ with coefficients in R such that

$$f(\underline{X} + \underline{Y}) = f(\underline{X}) + \sum_{j=1}^{n} \frac{\partial f}{\partial X_j}(\underline{X}) \cdot Y_j + \sum_{j=1}^{n} \sum_{k=1}^{n} \hat{h}_{jk}(\underline{X}, \underline{Y}) Y_j Y_k \ .$$

Note that also the partial derivatives have coefficients in R. Putting $Z_j = X_j + Y_j$ and $\underline{Z} = (Z_1, \ldots, Z_n)$ and defining $\tilde{h}_{jk}(\underline{X}, \underline{Z}) := \hat{h}_{jk}(\underline{X}\,,\, \underline{Z} - \underline{X})$, we obtain that

$$f(\underline{Z}) - f(\underline{X}) = \sum_{j=1}^{n} \frac{\partial f}{\partial X_j}(\underline{X}) \cdot (Z_j - X_j) + \sum_{j=1}^{n} \sum_{k=1}^{n} \tilde{h}_{jk}(\underline{X}, \underline{Z})(Z_j - X_j)(Z_k - X_k) \ . \quad (24.16)$$