

1. The Theory of Galois Extensions

1.1 The Galois Group

In the first two sections we will develop the algebraic foundations of the theory. The fields we are treating are not necessarily algebraic number fields of finite degree, and in fact can be taken to be arbitrary abstract fields. This is of some importance for our purposes as we will apply the results developed here also to \mathfrak{p} -adic fields. For simplicity, however, we will assume that the fields have characteristic 0.

Let us recall the following elementary facts. If K is a finite extension of F , say $K = F(\theta)$, where θ is a root of the irreducible polynomial $f \in F[X]$, and where f has the factorization

$$f(x) = (x - \theta)(x - \theta') \cdots (x - \theta^{(n-1)})$$

in the algebraic closure of F , then the fields

$$K, K' = F(\theta'), \dots, K^{(n-1)} = F(\theta^{(n-1)})$$

are called the conjugate fields of K over F . The map assigning to each element $\alpha = g(\theta)$ in K the element $\alpha^{(\nu)} = g(\theta^{(\nu)})$ in $K^{(\nu)}$ defines an isomorphism between K and $K^{(\nu)}$. For defining this isomorphism we needed a generating element θ and its conjugates; but θ is not at all uniquely defined by K . For this reason we now want to define the isomorphism in a way that does not depend on θ , and which makes the independence of the notion of an isomorphism from the choice of θ evident.

Definition 1. *A map from a field extension K of F to another field extension K' of F is called an isomorphism of K over F if the map*

1. *is injective*
2. *leaves elements of F fixed,*
3. *is a homomorphism, that is if $\alpha \circ \beta = \gamma$, where \circ denotes one of the four elementary operations, implies that $\alpha' \circ \beta' = \gamma'$.*

The maps from K onto the conjugates $K^{(\nu)}$ defined above are examples of such isomorphisms. We now have the following converse: If K has finite degree over F , then the n maps

$$K \longrightarrow K, \quad K \longrightarrow K', \quad K \longrightarrow K'', \quad \dots, \quad K \longrightarrow K^{(n-1)}$$

are the only isomorphisms of $K|F$. In fact: assume that we are given an isomorphism of $K|F$ and consider the image of a generator θ ; since θ is a root of the polynomial $f(x) \in F[X]$, we see that θ' satisfies the same equation since the coefficients of f all lie in F , hence are fixed by the isomorphism. Thus we have $f(\theta') = 0$, and this implies that θ' is a conjugate of θ . Moreover, if $\alpha = g(\theta)$ is an arbitrary element of K , then by condition (1.3) the element α must get mapped to $\alpha' = g(\theta')$. We have proved:

Theorem 2. *If $K|F$ is an algebraic extension of degree n , then K admits exactly n different isomorphisms over F , namely the maps from K to the n conjugates $K^{(\nu)}$.*

It can happen that some image field $K^{(\nu)}$ coincides with K . We define:

Definition 3. *An isomorphism of K over F onto itself is called an automorphism of K over F .*

Such automorphisms occur for extensions of finite degree when a field K coincides with one of its conjugates, that is, if $K = K^{(\nu)}$ as a set. Of course the isomorphism $K \longrightarrow K^{(\nu)}$ need not be the identity map sending every element to itself. This can be seen in the example

$$K = \mathbb{Q}(\sqrt{2}) \quad \text{and} \quad K' = \mathbb{Q}(-\sqrt{2}).$$

Here $K = K'$, and the map sending elements to their conjugates is an automorphism different from the identity.

We define next

Definition 4. *The extension $N|F$ is called normal or Galois if every isomorphism of N over F is an automorphism.*

By what we proved above this means that all conjugate fields $N^{(\nu)}$ coincide, hence

$$N = N' = \dots = N^{(n-1)}.$$

By Theorem 2 there are exactly n automorphisms. Thus we can state

Theorem 5. *An algebraic extension N of finite degree n over F is Galois if and only if all its conjugates with respect to F coincide. In this case there are exactly n automorphisms over F .*

We now want to derive a criterium that allows us to check computationally whether an extension N is normal. Representing N with a primitive element

θ , we can write $N = F(\theta)$; then all θ' must lie in N , which means that the $\theta^{(\nu)}$ can be expressed rationally by θ , and we have

$$\theta^{(\nu)} = g_\nu(\theta),$$

where the g_ν are polynomials with coefficients in F . Conversely, the existence of n such polynomials implies that the field N is normal. This is the desired rational criterium.

The notion of Galois extensions is of essential importance for the discussion of arbitrary fields. This is because every field K can be embedded into a normal extension. This can be seen as follows: if $K = F(\alpha)$ is an extension of F , where α satisfies the equation

$$f(X) = (X - \alpha)(X - \alpha') \cdots (X - \alpha^{(n-1)}),$$

then we claim that the field $N = F(\alpha, \alpha', \dots, \alpha^{(n-1)})$ is a normal extension of F containing K . Indeed: an isomorphism of N transforms the relation $f(\alpha) = 0$ into $f(\alpha^{(n-1)}) = 0$, hence the elements $\alpha, \dots, \alpha^{(n-1)}$ are only permuted. Thus although the order of the roots might change, the field they generate stays the same, hence is Galois. This shows that every field can be embedded into a normal field. At the same time we have seen that every splitting field (a field generated by adjoining all the roots of a polynomial in $F[X]$) is normal; and this holds without imposing any condition on the polynomial like irreducibility or reducibility. Thus we have

Theorem 6. *Every algebraic extension of finite degree $F(\alpha)$ of F can be embedded into a normal field of finite degree over F , namely the field $N = F(\alpha, \alpha', \dots, \alpha^{(n-1)})$ generated by all the conjugates of α .*

We now can define Galois groups. We interpret the automorphisms of a Galois extension $N|F$ as operations and denote them by letters σ, τ, \dots . Then we define the product $\sigma \cdot \tau$ to be the composition of σ and τ . The image of α under the map σ is denoted by α^σ , and we write $\alpha \mapsto \alpha^\sigma$. If τ is another automorphism, then we have

$$\alpha \xrightarrow{\sigma} \alpha^\sigma \xrightarrow{\tau} (\alpha^\sigma)^\tau = \alpha^{\sigma\tau}.$$

For a clearer formulation we now insert a group theoretic excursion. (We will develop our group theoretic tools only when needed, and the following section is just the first out of several excursions into group theory.)

We start with the

Definition 7. *A group G is a system of elements with a well defined multiplication with the following properties:*

- 1) *associativity: $a(bc) = (ab)c$;*
- 2) *Law of unlimited and unique division: the equations $ax = b$ and $ya = b$ have unique solutions for all $a, b \in G$.*

The law of commutativity is not required. If it holds, the group is called *commutative* or *abelian*.

Condition 2) may be replaced by

2a) There exists a unit element e (usually denoted by 1) such that

$$ea = ae = a$$

for all $a \in G$.

2b) The equation

$$ax = e$$

has a unique solution denoted by $x = a^{-1}$ ("inverse of a ").

There is no need to discuss the very simple proof of the equivalence between 7) on the one hand and 2a) and 2b) on the other hand, which can be found in any book on group theory.

We now can show that the automorphisms of a field N form a group.

1.) Assume that we are given automorphisms ρ, σ, τ and an element $\alpha \in N$. Then we can form two products from these three automorphisms:

$$(\rho\sigma)\tau \quad \text{and} \quad \rho(\sigma\tau).$$

We have to show that

$$(\alpha^{\rho\sigma})^\tau = (\alpha^\rho)^{\sigma\tau}.$$

We can achieve this as follows: by definition we have $\alpha^{\varphi\psi} = (\alpha^\varphi)^\psi$. Using this rule, the left hand side of the claimed equality becomes

$$\alpha \xrightarrow{\rho\sigma} \alpha^{\rho\sigma} = (\alpha^\rho)^\sigma \xrightarrow{\tau} ((\alpha^\rho)^\sigma)^\tau,$$

and the right hand side

$$\alpha^\rho \xrightarrow{\sigma\tau} (\alpha^\rho)^{\sigma\tau} = ((\alpha^\rho)^\sigma)^\tau.$$

Both results agree; this shows that our multiplication defined above is associative, that is, the first group property holds.

It remains to check 2a) and 2b). Since the identity map $\alpha \mapsto \alpha$ is an automorphism, there exists a unit element ε . In fact we have

$$\varepsilon\sigma = \sigma\varepsilon = \sigma,$$

$$\alpha \xrightarrow{\varepsilon} \alpha^\varepsilon \xrightarrow{\sigma} \alpha^{\varepsilon\sigma} = \alpha^\sigma, \quad \alpha \xrightarrow{\sigma} \alpha^\sigma \xrightarrow{\varepsilon} \alpha^{\sigma\varepsilon} = \alpha^\sigma.$$

2b) For every σ there is a σ^{-1} with $\alpha^\sigma \xrightarrow{\sigma^{-1}} \alpha$: in fact, we can define σ^{-1} to be the inverse map which switches the roles of preimage and image with respect to σ . This is clearly an automorphism, and we have

$$\alpha \xrightarrow{\sigma} \alpha^\sigma \xrightarrow{\sigma^{-1}} \alpha$$

i.e. $\sigma\sigma^{-1} = \varepsilon$.

This proves 2b), and we can collect our findings in

Theorem 8. *The automorphism group of a normal field N over F form a group G with respect to composition, called the Galois group of $N|F$. If N has finite degree n over F , then G has finite order n .*

Let us also make a few comments on the actual construction of the Galois group.

It is possible to describe the Galois group of $N|F$ if N is generated by the element θ , and if the substitutions existing between θ and its conjugates are known. Assume for example that we are given

$$f(X) = (X - \theta)(X - \theta') \cdots (X - \theta^{(n-1)}),$$

and that we know the polynomials g_ν with

$$\theta^{(\nu)} = g_\nu(\theta).$$

Let us introduce the notation

$$g_\nu(X) = g_\sigma(X)$$

for the conjugates, i.e. write

$$\theta^\sigma = g_\sigma(\theta);$$

similarly we have

$$\theta^\tau = g_\tau(\theta),$$

where τ is another automorphism; then we can determine the polynomial $g_{\sigma\tau}$ with

$$\theta^{\sigma\tau} = g_{\sigma\tau}(\theta).$$

In fact we have

$$\theta^{\sigma\tau} = (\theta^\sigma)^\tau = g_\sigma(\theta)^\tau.$$

Since g_σ is a polynomial with coefficients from F , which are invariant under τ , we only need replace θ by θ^τ , and we can conclude

$$\theta^{\sigma\tau} = g_\sigma(\theta^\tau) = g_\sigma(g_\tau(\theta)).$$

By checking which of the polynomials g_ν has the same value $g_\nu(\theta) = \theta^{\sigma\tau}$, we find the index ν resp. the automorphism ρ to which the product $\sigma\tau$ corresponds. In practice, one only has to compute compositions of polynomials. This composition is not necessarily commutative. We also remark that the equations are only valid for θ and are not identities that hold for all values of X , i.e. we do not have

$$g_{\sigma\tau}(X) = g_\sigma(g_\tau(X))$$

in general; we only have

$$g_{\sigma\tau}(X) \equiv g_{\sigma}(g_{\tau}(X)) \pmod{f(X)}$$

as a congruence in the polynomial ring $F[X]$. We will be content with these remarks on the explicit representation of the Galois group.

We also see that the Galois group need not be commutative, since $g_{\sigma}(g_{\tau}(\theta))$ need not coincide with $g_{\tau}(g_{\sigma}(\theta))$. If the commutative law is satisfied, however, then the extension $N|F$ is called abelian. If the Galois group is even cyclic, that is, if its elements are powers of a single automorphism, then $N|F$ is called cyclic.

The Galois group will turn out to be a universal invariant to which the properties of the field can be related. The simplification provided by group theory comes from the fact that the behavior of *infinitely* many elements of N under the action of automorphisms is described by the *finitely* many elements of G . On the one hand things are slightly complicated by the fact that the composition in G is, in contrast to the multiplication in N , not necessarily commutative. But experience has shown that calculations in the noncommutative realm are governed by simpler laws than in the commutative case since the multiformity due to switching factors is no longer present.

1.2 The Fundamental Theorem of Galois Theory

We begin with some group theory. Assume that we are given a group G with finitely or infinitely many elements. If a subset H of G has the properties of a group, we say that H is a subgroup of G . If H is a *finite* subset of G , checking that H is a subgroup of G requires only the verification of the following property: if a and b are elements of H , then so is ab . In fact, consider the powers of a ; since they all belong to H by assumption, there exist only finitely many different powers a^{ν} . But $a^{\nu} = a^{\mu}$ for $\nu > \mu$ implies $a^{\nu-\mu} = 1$, as well as $a \cdot a^{\nu-\mu-1} = 1$, or $a^{-1} = a^{\nu-\mu-1}$. Thus all the group axioms hold in H . We state this as

Theorem 9. *A finite subset H of a group G is a subgroup if and only if it is closed under multiplication.*

Each subgroup H of G induces an equivalence relation on G , for whose definition we first say that two elements a and b of G are right congruent with respect to the modulus H :

$$a \stackrel{r}{\equiv} b \pmod{H},$$

if the quotient ab^{-1} is in H , that is, if

$$ab^{-1} = h, \quad \text{i.e., } a = hb$$

for some $h \in H$.

Consider the following special case: let G be the additive group of integers, and let H consist of the multiples of the natural number m ; then

$$s \stackrel{r}{\equiv} t \pmod{H}$$

means that

$$s - t = g \cdot m$$

for some integer g , i.e., that we have, in the usual meaning of congruences in elementary number theory,

$$s \equiv t \pmod{m}.$$

Congruences modulo H therefore generalize the usual notion of congruence. This also gives us an example where the group operation is written additively.

We now show that the congruence relation defined above is an equivalence relation; this immediately implies that G is a union of disjoint cosets by collecting elements that are congruent or equivalent to each other.

An equivalence relation has to satisfy the following laws:

- 1) reflexivity;
- 2) symmetry;
- 3) transitivity.

In order to show that our congruence relation is an equivalence relation, we have to verify:

- 1) We have

$$a \stackrel{r}{\equiv} a \pmod{H}.$$

But this says only that $aa^{-1} = e$ should be an element of H . According to the definition, every group contains the unit element, which at the same time is contained in every subgroup. Thus 1) is satisfied.

- 2) From

$$a \stackrel{r}{\equiv} b \pmod{H} \text{ it follows that } b \stackrel{r}{\equiv} a \pmod{H}.$$

By definition, $a \stackrel{r}{\equiv} b \pmod{H}$ means that $ab^{-1} = h$ for some $h \in H$. We have to show that $ba^{-1} \in H$. But since

$$ba^{-1} = (ab^{-1})^{-1} = h^{-1},$$

and since H contains with h also h^{-1} , we have 2).

- 3) From

$$a \stackrel{r}{\equiv} b \pmod{H} \quad \text{and} \quad b \stackrel{r}{\equiv} c \pmod{H} \quad \text{follows} \quad a \equiv c \pmod{H}.$$

The proof is almost trivial, since

$$\begin{array}{lll} a \stackrel{r}{\equiv} b \pmod{H} & \text{means} & ab^{-1} = h \in H, \\ b \stackrel{r}{\equiv} c \pmod{H} & \text{means} & bc^{-1} = h' \in H. \end{array}$$

Multiplying these two equations gives

$$ab^{-1}bc^{-1} = ac^{-1} = hh' \in H,$$

since with h and h' the group H also contains their product.

The subdivision of G into classes (which will be called *cosets* in the following) is accomplished by collecting all elements equivalent to an element g into the same coset. We now get the elements equivalent to g by multiplying g from the left with elements of H , and we can denote this symbolically by writing Hg for this coset. The element g is called a representative of the coset Hg . We can write symbolically

$$G = \sum_i Hg_i,$$

where the g_i form a complete set of representatives of the cosets. In words: G is the disjoint union of these cosets.

The number of different cosets, called the index of H in G , is denoted by $j = [G : H]$. Informally speaking, the index tells us how much bigger G is than H . If, in particular, G has finite order n , and if m denotes the order of H , then we have $n = j \cdot m$. In fact, every coset has m elements (since $hg = h'g$ implies $h = h'$), and since there are j cosets, whose elements are pairwise different, we see that G has exactly $n = jm$ elements as claimed. In particular we have: the order of H divides the order of G .

If a is the element of an arbitrary group G , then the powers of a , namely $e = a^0, a^{\pm 1}, a^{\pm 2}, \dots$ form a subgroup H of G . If this subgroup is finite, say of order f , then it is easily seen that the elements of H are

$$e = a^0, a^1, \dots, a^{f-1},$$

and we have $a^f = e$. Here f is called the order of a ; it clearly divides the order of the group G .

In the special case where H only consists of the unit element (which forms a group we will denote by 1), the number of cosets equals n , since the cosets consist of single elements, as is easily seen: $a \equiv b \pmod{1}$ implies $a = b$. We have $m = 1$, and the order of G can be expressed as

$$n = [G : 1];$$

this will be used later.

These group theoretical results can be applied to the investigation of the structure of normal extensions.

For the rest of this section, fix a normal extension N of finite degree n over the base field F and its Galois group G . Our goal is studying the fields between N and F . We want to find a relation between the subextensions $E|F$ of $N|F$ and the subgroups H of G . We will show that there is a bijection between these objects. This is the main content of Galois theory.

We start by defining two maps:

a) a map assigning to each subextension $E|F$ a subgroup H , which will be denoted by $E \longrightarrow H$.

The subgroup H will contain all automorphisms of N (that is, elements of G) that not only fix the elements of F but also those of E . Then H is a group and thus a subgroup of G . In fact, if φ and ψ are automorphisms in H , then the products $\varphi\psi$, $\varphi\psi^{-1}$ and $\psi^{-1}\varphi$ fix the elements of E . We also claim that H is the Galois group of $N|E$: in fact, N is normal over E since every automorphism of $N|E$ is also an automorphism of $N|F$.

b) Similarly we can define a map $H \longrightarrow E$ sending subgroups H to certain subextensions $E|F$: the field E consists of all elements of N that are fixed by the automorphisms in H . Note that E is a field and thus a subextension of $N|F$: this is because if $\alpha, \beta \in E$, then so is $\alpha \circ \beta$, where “ \circ ” is any of the four field operations. This can be seen as follows: let φ be an automorphism fixing α and β , i.e., with $\alpha^\varphi = \alpha$ and $\beta^\varphi = \beta$. Then

$$(\alpha \circ \beta)^\varphi = \alpha^\varphi \circ \beta^\varphi,$$

since φ is a map preserving rational relations; thus

$$(\alpha \circ \beta)^\varphi = \alpha \circ \beta$$

for all $\varphi \in H$. Since the elements of F are fixed under the action of G , this holds a fortiori for the action of H . All this shows that E is a subfield of N containing F as a subfield.

The two maps

$$H \longrightarrow E, \quad E \longrightarrow H$$

were defined independently from each other, and it is a priori not at all clear that they are part of one and the same bijective relation, i.e., that

$$\begin{aligned} \text{if } H \longrightarrow E, E \longrightarrow H' \quad \text{then } H &= H', \\ \text{if } E \longrightarrow H, H \longrightarrow E' \quad \text{then } E &= E'. \end{aligned}$$

For now, all we can say is

Theorem 10. a) If E is a subextension of $N|F$, then the automorphisms of G fixing the elements of E form a subgroup H of G , the stabilizer of E . This group is also the Galois group of $N|E$.

b) If H is a subgroup of G , then the elements of N invariant under all automorphisms of H form a subfield E of N containing F , called the fixed field of H .

It follows from a) that the group assigned to the base field F is the Galois group G itself: $F \longrightarrow G$; in fact, G fixes all elements of F . Moreover the element ε as a group 1 fixes all elements of N , hence we have $1 \longrightarrow N$. We can express these facts in the following way:

$$\begin{array}{ccc} N & \longrightarrow & 1 \\ E & \longrightarrow & H \\ F & \longrightarrow & G \end{array} \quad \begin{array}{ccc} 1 & \longrightarrow & N \\ H & \longrightarrow & E \\ G & \longrightarrow & ? \end{array},$$

where for now both columns are independent from each other, and where the question mark remains to be taken care of; currently we can't say anything about it. We will be able to give an answer only after we have proved the fundamental theorem of Galois theory, which states the following:

- a) If $E \longrightarrow H$, then $H \longrightarrow E$; and conversely:
 b) if $H \longrightarrow E$, then $E \longrightarrow H$.

This immediately implies that the two mappings of Theorem 10 can be subsumed into a single bijection; in particular, we can answer the question above: we have $G \longrightarrow F$.

a) Assume that we are given the correspondence $E \longrightarrow H$; then we have to show that $H \longrightarrow E$. We know that we can assign a unique subextension $E'|F$ to the group H , and it remains to show that $E = E'$. In order to do this we go one step further and exploit the fact that we can assign the group H' to the field E' ; thus we get a chain of maps

$$E \longrightarrow H \longrightarrow E' \longrightarrow H',$$

which we have to study now. As a first step we will show that, in the direction of the arrows, the objects cannot get smaller, in other words: that the sequence implies

$$E \subseteq E', \quad H \subseteq H'.$$

This follows by *purely formal* arguments: E' is the set of all elements fixed by the automorphisms in H (by definition of E'). The elements of E are fixed under H by assumption, hence E' contains E , i.e. $E \subseteq E'$.

We can argue similarly for the subgroups: by definition H' contains all automorphisms fixing the elements of E' , and H does fix all all elements of E' , hence we have $H \subseteq H'$.

Thus we have found the following relations:

$$N \supseteq E' \supseteq E \supseteq F, \tag{1.1}$$

$$1 \subseteq H \subseteq H' \subseteq G. \tag{1.2}$$

The fact that the inclusions are reversed allows us now to finish the proof by using arguments involving the degree of fields and the index of groups:

$$\begin{aligned} (1.1) \text{ implies:} & \quad [N : E] \geq [N : E'], \\ (1.2) \text{ implies:} & \quad [H : 1] \leq [H' : 1]. \end{aligned}$$

Now we exploit the fact that H is the Galois group of N over E , i.e., that

$$[H : 1] = [N : E],$$

and, similarly,

$$[H' : 1] = [N : E'].$$

Together with the preceding inequalities we find that

$$[H : 1] = [H' : 1]$$

and

$$[N : E] = [N : E'];$$

Thus the identity

$$[N : E] = [N : E'][E' : E]$$

implies immediately $[E : E'] = \varepsilon$, and since $E' \supseteq E$ we get

$$E = E'.$$

b) The proof of the converse cannot be done in a completely analogous manner. We work only with

$$H \longrightarrow E \longrightarrow H'$$

and have to show that

$$H = H'.$$

Again we have $H \subseteq H'$. If we can show that

$$[H : 1] \geq [H' : 1],$$

then the claim $H = H'$ will follow. This inequality will be derived using a primitive element θ of N over F by constructing the function

$$g(X) = \prod_{\varphi \in H} (X - \theta^\varphi).$$

Since g is symmetric in *those* conjugates corresponding to the group H , the coefficients are invariant under the automorphisms from H . More exactly: if ψ is any automorphism in H , then

$$g^\psi(X) = \prod_{\varphi \in H} (X - \theta^\varphi)^\psi = \prod_{\varphi \in H} (X - \theta^{\varphi'}) = g(X),$$

where $\varphi' = \varphi\psi$. In fact, the product $\varphi\psi$ runs over the elements of the group H exactly once if φ does. Thus we have shown that $g(X)$ is invariant under the action of H , i.e., that its coefficients are elements of N fixed by H ; but this characterizes the elements of E ; thus $g(X)$ is a polynomial in $E[X]$. But now $F(\theta) = N$ implies $E(\theta) = N$, i.e., θ is also a primitive element for N over E . Since θ is the root of a polynomial $g(X)$ of degree $[H : 1]$, we deduce that

$$[N : E] \leq \deg g(X) = [H : 1].$$

But since H' is the Galois group of $N|E$, that is, since $[N : E] = [H' : 1]$, we find

$$[H' : 1] \leq [H : 1],$$

which is what we wanted to prove.

Since the maps between the subgroups of G and the subextensions of $N|F$ have now been shown to be a bijection, we will introduce the notation

$$E \longleftrightarrow H.$$

In particular this result shows that $G \longrightarrow F$. This is not at all trivial; it says: *Only* the elements in F are invariant under all the automorphisms of $N|F$, or

$$\alpha = \alpha^\sigma \quad \text{for all } \sigma \in G$$

holds if and only if $\alpha \in F$.

Theorem 11. *If*

$$E \longrightarrow H \quad \text{then} \quad H \longrightarrow E, \quad (1.3)$$

$$H \longrightarrow E \quad \text{then} \quad E \longrightarrow H. \quad (1.4)$$

Thus the two maps $E \longrightarrow H$ and $H \longrightarrow E$ can be subsumed into one and the same bijective correspondence

$$E \longleftrightarrow H$$

between the subextensions $E|F$ of $N|F$ and the subgroups H of G .

This fundamental fact is called the Fundamental Theorem of Galois Theory. It gives a complete description of the (at least at first) somewhat obscure set of subextensions of $N|F$. In particular we find that there are only finitely many such subextensions, since a finite group obviously only has finitely many subgroups. In order to characterize all subextensions, one has to come up with a list of all subgroups, which can be done for any given example in finitely many steps. We also get a whole series of corollaries, which all can be seen as additions to the fundamental theorem.

First we have:

$$E \supseteq E' \quad \text{if and only if} \quad H \subseteq H'.$$

This result can be formulated by saying the bijection between fields and groups is inclusion reversing. This is immediately clear: let $E' \supseteq E$ and $E' \longleftrightarrow H'$, $E \longleftrightarrow H$, i.e., H is the group of all automorphisms fixing the elements of E , and H' is the group of all automorphisms fixing the elements of E' . In particular, H' fixes the elements of E because E is contained in E' , and this means that we must have

$$H' \subseteq H.$$

Conversely, assume that

$$H' \subseteq H;$$

then E' consists of all elements fixed by H' ; now E consists of all elements fixed by H , hence these elements of E are also fixed by H' : this is because the elements of H' are all contained in H . This implies

$$E' \supseteq E.$$

We now study some degree and index relations. If we are given a bijection in the above sense

$$N \longleftrightarrow 1, \quad E \longleftrightarrow H, \quad F \longleftrightarrow G,$$

then we have

$$[N : E] = [H : 1],$$

where H is the Galois group of $N|E$. This equality and

$$[N : F] = [G : 1]$$

imply that

$$[E : F] = [G : H].$$

If we have more than one intermediate field,

$$N \longleftrightarrow 1, \quad E' \longleftrightarrow H', \quad E \longleftrightarrow H, \quad F \longleftrightarrow 1,$$

then the results above show that

$$[N : E] = [H : 1],$$

and similarly, by taking E' as the intermediate field,

$$[N : E'] = [H' : 1].$$

If we have $E' \supseteq E$ and $H' \subseteq H$, which, according to what we have proved, are equivalent conditions, then

$$[N : E] = [N : E'][E' : E]$$

and

$$[H : 1] = [H' : E][H : H'].$$

Since the left hand sides and the first factors on the right hand sides agree, the second factors must coincide, and we have

$$[E' : E] = [H : H'].$$

We collect everything in

Theorem 12. *If E is associated to the subgroup H , then*

$$\begin{aligned} [N : E] &= [H : 1], \\ [E : F] &= [G : H]. \end{aligned}$$

Moreover: if E is associated to the subgroup H and E' to the subgroup H' , then the relations

$$E \subseteq E' \quad \text{and} \quad H' \subseteq H$$

are equivalent, and in this case we have

$$[E' : E] = [H' : H].$$

We now want to translate the relation of being conjugate (on the side of subfields of N over F) into a relation between groups.

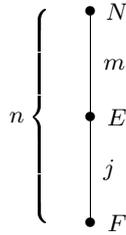


Fig. 1.1.

From the elementary theory of algebraic extensions we know the following. If $F \subseteq E \subseteq N$ is a field tower, $[E : F] = j$, $[N : E] = m$, $[N : F] = n$, that is, $n = jm$, then the n conjugates of some $\alpha \in N$ can be arranged into j lines of m numbers in such a way that the numbers in any line are conjugate with respect to E or to a field conjugate to E . If α lies in E , then the numbers in a line are always equal to each other. If α is a primitive element of E over F ,

then the numbers in the different lines are pairwise different and represent exactly the different conjugates of α with respect to F . If $N|F$ is Galois, then this can be expressed as follows: as an element of E , α is invariant under H . As a primitive element of E , α is fixed *only* by H (i.e., by no strictly bigger subgroup of G); we say that α is a number belonging to H .

We now apply all the automorphisms of G to α by first decomposing G as follows:

$$G = \sum_{i=1}^j H\sigma_i,$$

where the σ_j run through a full set of right representatives of G/H ; then

$$\alpha^{H\sigma_j} = \alpha^{\sigma_j},$$

since α is fixed by H . Of course the last expression means that for all $\rho \in H$ we have $\alpha^\rho = \alpha$. The α^{σ_j} are pairwise distinct since there are j different conjugates. Thus there are as many conjugates of α with respect to N as there are cosets modulo H .

Before we state something similar for the field E and its conjugates $E^{(\nu)}$, we will insert another group theoretic excursion. If H is a subgroup of G and g any element of G , then we can consider

$$g^{-1}Hg. \tag{1.5}$$

We claim: (1.5) is a group isomorphic to H . In fact, the elements $h, h' \in H$ correspond to the elements $g^{-1}hg$ and $g^{-1}h'g$ in (1.5). The fact that this map between the group H and the system (1.5) transformed by g is a bijective homomorphism follows from the law of unlimited and unique division (see page 3): the map in the direction

$$H \longrightarrow g^{-1}Hg$$

is trivially well defined; but so is its converse, since

$$g^{-1}hg = g^{-1}h'g$$

implies

$$h = h'$$

by multiplying with g from the left and with g^{-1} from the right. And since moreover we have

$$hh' \longmapsto g^{-1}hgg^{-1}h'g = g^{-1}hh'g,$$

the isomorphism between H and $g^{-1}Hg$ is established, as we have shown that the product of the images is equal to the image of the products.

Thus the transformation (1.5) gives us a map onto an isomorphic subgroup called a *subgroup conjugate to H in G* .

Now we ask how many such conjugate subgroups there are, in other words: which g yield the same conjugate subgroup $g^{-1}Hg$? The answer depends only on the coset modulo H to which g belongs. In fact, if

$$g' \stackrel{r}{\equiv} g \pmod{H},$$

i.e.,

$$g' = hg$$

for some $h \in H$, then

$$(hg)^{-1}Hhg = g^{-1}h^{-1}Hhg,$$

(since $(hg)^{-1} = g^{-1}h^{-1}$, as can be seen from $g^{-1}h^{-1}hg = e$) and since

$$h^{-1}Hh = H$$

(since $h \in H$), we find

$$(hg)^{-1}Hhg = g^{-1}Hg.$$

Thus there are at most as many conjugate subgroups as there are cosets modulo H . The resulting subgroups, however, need not necessarily be pairwise distinct; if, for example, G is abelian, then they all coincide.

Let us now return to Galois theory and ask for the groups associated to the conjugate fields $E^{(\nu)}$ of a subextension $E|F$ of $N|F$, then we are led to the following assertion: if we are given

$$E \longleftrightarrow H \quad \text{and} \quad E' \longleftrightarrow H',$$

and if E' is a subfield of N conjugate to E , then this is equivalent to the fact that H' is conjugate to H in G .

In fact, conjugate fields E, E' are, according to the results from Section 1.1, of the type

$$E = F(\alpha), \quad E' = F(\alpha'),$$

where α' is a conjugate of α . Here, where α and α' lie in the normal field N , we can write $\alpha' = \alpha^\sigma$ for a suitable $\sigma \in G$, hence

$$E = F(\alpha), \quad E^\sigma = F(\alpha^\sigma),$$

where the exponent of E indicates that the automorphism σ is to be applied to every element of E . The fact that the elements of E^σ are fixed by $\sigma^{-1}H\sigma$ can be seen from the equation

$$(\alpha^\sigma)^{\sigma^{-1}H\sigma} = \alpha^{H\sigma} = \alpha^\sigma,$$

or directly from

$$(E^\sigma)^{\sigma^{-1}H\sigma} = E^{H\sigma} = E^\sigma.$$

This equation has to be interpreted elementwise, that is as an equation valid for every element of E . If, conversely, the elements of E^σ are fixed under some automorphism τ from G :

$$(E^\sigma)^\tau = E^\sigma,$$

then applying σ^{-1} shows

$$E^{\sigma\tau\sigma^{-1}} = E.$$

Thus $\sigma\tau\sigma^{-1}$ fixes the elements of E , hence belongs to H , say $\sigma\tau\sigma^{-1} = \varphi$ for $\varphi \in H$. This implies $\tau = \sigma^{-1}\varphi\sigma$, i.e., τ belongs to $\sigma^{-1}H\sigma$. Thus $\sigma^{-1}H\sigma$ is the exact invariant group of E^σ . We have proved:

Theorem 13. *If*

$$E \longleftrightarrow H,$$

then for every automorphism $\sigma \in G$ we have

$$E^\sigma \longleftrightarrow \sigma^{-1}H\sigma.$$

Let us now emphasize a result obtained above. If the subfield E between F and N has degree j and if $E = F(\alpha)$, then we have seen that there exist exactly j conjugates of α , and that these can be written in the form α^{σ_i} ($i = 1, \dots, j$), where

$$G = \sum_{i=1}^j H\sigma_i$$

is a right coset decomposition of G modulo H . The maps from E to the fields $E^{\sigma_i} = F(\alpha^{\sigma_i})$ give us j isomorphisms of E fixing the elements of F . All these maps come from automorphisms of the normal extension N . But since, according to Theorem 2, E has only j isomorphisms, these are *all* isomorphisms of $E|F$. Thus the automorphisms of N yield all isomorphisms of E . We state this as

Theorem 14 (Baer's Lemma). *If E is a subextension of $N|F$ and if E' is isomorphic to E , then E' also is a subextension of $N|F$ and arises from E by an application of some automorphism σ of $N|F$.*

Conversely, for every $\sigma \in G$ the field E^σ will be isomorphic to E over F . In the modern theory of algebraic extensions, Baer's Lemma is put at the beginning, and it is proved without using the existence of a primitive element for E . Using this lemma the theorems of Galois theory are then proved without having to resort to the generators θ of the corresponding fields. Such an arrangement of the proofs can be found in the appendix to Steinitz's famous work on the theory of abstract fields (edited by Baer and Hasse, and furnished with appendices on Galois theory).

We now want to discuss another notion of group theory, namely the one that corresponds to the *normal* subextensions $E|F$ in the same way as the notion of conjugate subgroups corresponds to conjugate subfields $E^{(\nu)}$. Let H be a subgroup of G ; then $g^{-1}Hg$ are the subgroups conjugate to H . If all conjugate subgroups of H coincide, i.e., if $g^{-1}Hg = H$ for all $g \in G$, then H is called a normal (or invariant) subgroup of G . (Of course this has to be interpreted as an equality of sets, not as an equality of elements $g^{-1}hg = h$ for all $h \in H$. The latter only holds if H is an abelian subgroup, because then $hg = gh$. In general, if the elements of H are given by the sequence

$$h_1, \dots, h_m,$$

then the sequence

$$g^{-1}h_1g, g^{-1}h_2g, \dots, g^{-1}h_mg$$

will be a permutation of the first.)

An immediate consequence of the property of normality can be read off the relation $Hg = gH$. Just as we have defined the right equivalence relation

$$a \stackrel{r}{\equiv} b \pmod{H}$$

by " $ab^{-1} \in H$ ", we can define a left equivalence relation

$$a \stackrel{l}{\equiv} b \pmod{H}$$

by $a^{-1}b \in H$, and this relation has analogous properties; in particular, G can be decomposed into left cosets

$$G = \sum_{i=1}^j g_i H.$$

The fact that H is normal means that the decompositions into left and right cosets coincide, since $g^{-1}Hg = H$ is equivalent to $Hg = gH$. Moreover, the normality condition $Hg = gH$ guarantees that we can work with residue classes in the usual way, i.e., that the product of two residue classes can be defined as the residue class of the product of elements representing the classes. This shows that the cosets modulo a normal subgroup H of G form a group. In fact, if we have

$$a \stackrel{r}{\equiv} b \pmod{H},$$

then $ab^{-1} = h$ for some $h \in H$, or $a = hb$. From this we see that, even if H is not normal, multiplication of a right congruence $a \stackrel{r}{\equiv} b \pmod{H}$ with an element c from the right leads to a well defined coset Hbc (or $Hac = Hbc$), because multiplication by c gives the equation $ac = hbc$, which means

$$ac \stackrel{r}{\equiv} bc \pmod{H}.$$

In order to arrive at a well defined multiplication of cosets by multiplying representatives, we should be able to multiply from the left by c , which is, however, not always allowed.

In fact,

$$ca \stackrel{r}{\equiv} cb \pmod{H}$$

means that $ca = hcb$ for some $h \in H$. This holds since $a = h'b$ for some $h' \in H$ whenever $bh' = hb$. Such an equality would have to hold for every c and h' for a suitable $h \in H$. This implies the condition $Hc \subseteq cH$ for every c , in particular for c^{-1} , so we find $Hc^{-1} \subseteq c^{-1}H$ and $cH \subseteq Hc$. These two equations imply

$$Hc = cH.$$

Thus if H is normal in G , then $a \equiv b \stackrel{r}{\equiv} H$ implies

$$ca \stackrel{r}{\equiv} cb \pmod{H}.$$

Assume that this is the case, and let two cosets A and B modulo H be given with representatives $a, a' \in A_1$ and $b, b' \in B$, i.e.

$$a \stackrel{r}{\equiv} a' \pmod{H},$$

$$b \stackrel{r}{\equiv} b' \pmod{H}.$$

We now ask whether

$$ab \stackrel{r}{\equiv} a'b' \pmod{H}. \quad (1.6)$$

Multiplying the first equation from the right with b and the second from the left with a' we get

$$ab \stackrel{r}{\equiv} a'b \pmod{H},$$

$$a'b \stackrel{r}{\equiv} a'b' \pmod{H}.$$

These two equations imply our conjecture (1.6). Now that we know that the multiplication of cosets with respect to a normal subgroup is well defined, we only need to verify the existence of a unit element and of inverses: this will show that the cosets modulo a normal subgroup form a group. Let us do this now. As the unit we may take H ; in fact, multiplying any coset $Hg = gH$ with H from the left or the right yields the same coset $Hg = gH$ because of $HH = H$. Next, multiplying $Hg = gH$ for any g with $g^{-1}H = Hg^{-1}$ gives $Hgg^{-1}H = H$, hence $g^{-1}H = Hg^{-1}$ is the inverse of $Hg = gH$. Now we have verified that the cosets modulo H form a group. This group of cosets modulo some normal subgroup H is called the *factor group* of G modulo H and is denoted by G/H .

If in particular G is a *finite group*, then so is G/H , and the order of the factor group equals the index of H in G :

$$[G/H : 1] = [G : H].$$

Now let us apply this to Galois theory. Assume that we are given towers of fields and groups with

$$N \longleftrightarrow 1, \quad E \longleftrightarrow H, \quad F \longleftrightarrow G.$$

If $E|F$ is Galois, then we may expect that this is equivalent to “ H is normal in G ”. In fact, “ E is normal over F ” means that every isomorphism of E over F is an automorphism. By Baer’s Lemma, all fields conjugate to E over F have the form E^σ . Since the field E^σ corresponds to the group $\sigma^{-1}H\sigma$, the following two claims are clearly equivalent:

$$\begin{aligned} E^\sigma &= E \quad \text{for all } \sigma, \\ \sigma^{-1}H\sigma &= H \quad \text{for all } \sigma. \end{aligned}$$

This proves the conjecture. For this reason, Galois extensions are also called normal.

Now if we are given a normal subextension $E|F$ of $N|F$, then it has a Galois group H_0 whose order equals the degree of E over F , hence is equal to the index of H in G . This is also the order of the factor group G/H . The fact that they have the same order suggests that the Galois group H_0 of $E|F$ and the factor group G/H are isomorphic. Now E is fixed by H , that is the elements of E are fixed by the automorphisms in H . On the other hand the factor group consists of classes $H\sigma$, which yield all automorphisms of $E|F$ because the automorphisms from a single coset all give the same automorphism of E . Thus the number of the automorphisms of E that we have found equals its degree. Therefore these are *all* automorphisms of $E|F$, hence we have a bijection between H_0 and G/H . We can even show that this bijection is an isomorphism. For if we are given two automorphisms φ_1, φ_2 of $E|F$, and if $H\sigma_1$ and $H\sigma_2$ are the two corresponding cosets in the factor group G/H , then on the one hand $\varphi_1 \cdot \varphi_2$ is the automorphism of $E|F$ given by composing φ_1 and φ_2 , on the other hand $H\sigma_1\sigma_2$ equals $H\sigma_1 \cdot H\sigma_2$ (see page 19), and this representation shows that these automorphisms too are given by the composition of the automorphisms of $H\sigma_1$ and those of $H\sigma_2$. Thus the coset corresponding to the automorphism $\varphi_1 \cdot \varphi_2$ really is $H\sigma_1\sigma_2$. Collecting everything we have

Theorem 15. *If*

$$E \longleftrightarrow H,$$

then E is normal over F if and only if H is normal in G ; in this case, the Galois group of $E|F$ is isomorphic to the factor group G/H and its automorphisms arise by applying the cosets of G/H to E .

The laws contained in the fundamental theorem of Galois theory as well as the consequences we have developed can be represented graphically in a concise way. We can attach a graph to every extension as follows: as vertices we take the fields, and these are connected by an edge if one is contained in

the other. Numbers next to the edges denote the relative degrees. By coloring edges we can indicate whether fields are conjugate with respect to some base field, hence such a graph encodes everything we would like to know about such fields. We will often use this device below. In a similar way we can make up graphs for the Galois groups, and then the fundamental theorem of Galois theory asserts that the graphs of fields and groups are identical except for a reversion of inclusions.

The relations of inclusion, degree, index and being conjugate between the subextensions of $N|F$ together form the structure of $N|F$. The content of the fundamental theorem of Galois theory is the statement that the structure of $N|F$ corresponds uniquely to the structure of the Galois group G of $N|F$, and that one can be read off from the other.

We now deduce two consequences from the fundamental theorem. Assume that we are given the fields E_1, \dots, E_r ; the set of all elements contained in each of the fields E_1, \dots, E_r is called the *intersection* E of E_1, \dots, E_r .

E is also a field, because if α and β are contained in each of the fields E_1, \dots, E_r , then so do $\alpha \circ \beta$, where "o" again denotes one of the four operations in the field. We write

$$E = E_1 \cap E_2 \cap \dots \cap E_r.$$

If all E_1, \dots, E_r are intermediate fields between N and F , then we can consider the groups H_i associated to the E_i , and the inclusion relations imply that the intersection E corresponds to the *compositum*

$$H = H_1 \cdots H_r$$

of the subgroups, which by definition is the smallest subgroup of G containing all the H_i .

Conversely, the smallest subfield K of N containing all E_i as subfields is called the compositum of E_1, \dots, E_r . This field K must contain all rational compositions of the elements of E_1, \dots, E_r ; since these compositions already form a field K , every field containing E_1, \dots, E_r must be an extension of K ; in this sense K is the smallest such field, which we denote by

$$K = E_1 \cdots E_r.$$

Under the Galois correspondence, the inclusion relations show that the field K is associated to the *largest* subgroup of G contained in all the H_1, \dots, H_r , that is, to the intersection $H_1 \cap \dots \cap H_r$. In all these relations we have to observe that the intersection (of fields and groups) coincides with the set theoretic intersection, but that the compositum in general is *bigger* than the set theoretic union.

Theorem 16. *If*

$$E_1 \longleftrightarrow H_1, \dots, E_r \longleftrightarrow H_r,$$

then

$$E_1 \cdots E_r \longleftrightarrow H_1 \cap \cdots \cap H_r$$

and

$$E_1 \cap \cdots \cap E_r \longleftrightarrow H_1 \cdots H_r.$$

We now want to apply this result to *abelian extensions*. To this end assume that $N|F$ is abelian with abelian Galois group G . Recall the main theorem on abelian groups. It states that we can find elements ρ_1, \dots, ρ_s (possibly in many ways) in G such that every element $\sigma \in G$ can be written uniquely as

$$\sigma = \rho_1^{r_1} \cdots \rho_s^{r_s}, \quad (1.7)$$

where the r_i are integers uniquely determined modulo certain prime powers $p_i^{a_i}$ (the orders of the ρ_i). We say that G is the *direct product*

$$G = Z_1 \times \cdots \times Z_r, \quad Z_i = \{\varepsilon, \rho_i, \rho_i^2, \dots, \rho_i^{p_i^{a_i} - 1}\}.$$

of the Z_i . Using this fundamental theorem on abelian groups we now want to determine the structure of abelian fields. To this end we define

$$G_i = Z_1 \times \cdots \times Z_{i-1} \times Z_{i+1} \times \cdots \times Z_s,$$

that is, G_i consists of those σ for which, in the basis representation (1.7), we have $r_i \equiv 0 \pmod{p_i^{a_i}}$, so that we get

$$G = Z_i \times G_i \quad (i = 1, \dots, s).$$

Moreover we define the field N_i by

$$N_i \longleftrightarrow G_i;$$

since the intersection of all G_i clearly is the trivial group, Theorem 16 shows that

$$N = N_1 \cdots N_s.$$

This is the decomposition of N that we were looking for.

The Galois group of $N_i|F$ is, according to Theorem 15, the factor group G/G_i . We claim that it is isomorphic to Z_i :

$$G/G_i \simeq Z_i \quad (i = 1, \dots, s).$$

Both groups have the same order, since G/G_i does have $p_i^{a_i}$ elements, as can be seen from the basis representation for the elements of G_i , which shows that their cardinality is $n/p_i^{a_i}$. Since G can also be written in the form

$$G = \varepsilon G_i + \rho_i G_i + \dots + \rho_i^{p_i^{a_i} - 1} G_i,$$

we deduce without problems that computations with the cosets can be reduced to computations with the elements of Z_i , and the claim follows.

Thus $N_i|F$ is an extension whose Galois group is isomorphic to Z_i . But Z_i is cyclic of order $p_i^{a_i}$, hence so is N_i . Thus we have found that the field N can be written as the compositum of cyclic extensions N_i .

We now want to show that the components N_i of the compositum $N = N_1 \cdots N_s$ are, in a certain sense, *independent*: in fact we claim that the intersection of each of these fields with the compositum of the others equals F . For a proof we introduce

$$E_i = N_1 \cdots N_{i-1} N_{i+1} \cdots N_s;$$

then

$$E_i \longleftrightarrow G_1 \cap \cdots \cap G_{i-1} \cap G_{i+1} \cap \cdots \cap G_s = Z_i.$$

The last equality can again be deduced from the basis representation (1.7): in order that $\sigma = \rho_1^{a_1} \cdots \rho_s^{a_s}$ belong to this intersection it is necessary and sufficient that $a_k \equiv 0 \pmod{p_k^{a_k}}$ for all $k \neq i$, and this characterizes Z_i . Now $Z_i G_i = G$ (even as a direct product), hence

$$G = Z_i \cdot G_i \longleftrightarrow E_i \cap N_i,$$

and this means that

$$E_i \cap N_i = F$$

Thus we have proved:

Theorem 17. *The decomposition of the Galois group of an abelian extension $N|F$ into a direct sum of cyclic groups of prime power order $p_i^{a_i}$ corresponds to writing $N|F$ as a compositum of independent cyclic extensions $N_i|F$ of prime power degree, i.e., we have*

1. $N = N_1 \cdots N_s$,
2. $N_i \cap E_i = F$,

where E_i is the compositum of the $N_j \neq N_i$.

At the end of this section we want to investigate how the structure theorems of $N|F$ change if we replace the base field F by some larger field $\overline{F} \subseteq F$. Here we do not want to assume that \overline{F} is a subfield of N , but also allow that \overline{F} contains elements not lying in N . Of course instead of N we then have to consider the uniquely determined compositum $\overline{N} = N\overline{F}$ inside the algebraic closure of \overline{F} . Since the elements common to N and \overline{F} will be important, we set $E = N \cap \overline{F}$. Then $E \supseteq F$. We expect to find the structure indicated by Figure 1.2, in particular the relation $[N : E] = [\overline{N} : \overline{F}]$ between the degrees. We immediately see that \overline{N} is normal over \overline{F} . In fact, if θ is a primitive element of $N|F$, then θ clearly is primitive for $\overline{N}|\overline{F}$. But since $N|E$ is normal, all conjugates of θ belong to N ; thus they also belong to \overline{N} , and this shows that $\overline{N}|\overline{F}$ is indeed normal. Now let f denote the minimal polynomial of θ

in E , \bar{f} its minimal polynomial over \bar{F} . Then $\bar{f} \mid f$, since \bar{f} has a root in common with f . On the other hand, \bar{f} is not only a polynomial in \bar{F} but also in N . In fact, we have

$$\bar{f}(x) = \prod_{\varphi} (x - \theta^{\varphi}),$$

where the product is over all automorphisms φ of $\bar{N}|\bar{F}$; every linear factor of \bar{f} , hence \bar{f} itself, belongs to N . Thus \bar{f} belongs to E , and for the same reason as above we have $f \mid \bar{f}$, hence

$$\bar{f}(x) = f(x).$$

This implies that indeed $[N : E] = [\bar{N} : \bar{F}]$.

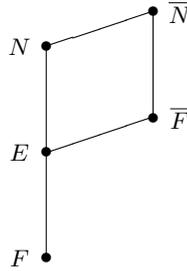


Fig. 1.2.

In the special case where \bar{F} has finite degree over E we remark that if $g = [\bar{F} : E]$, then $g = [\bar{N} : N]$, because in this case $[\bar{N} : E]$ is finite too, and we have $[\bar{N} : E] = [\bar{N} : N][N : E]$ as well as $[\bar{N} : E] = [\bar{N} : \bar{F}][\bar{F} : E]$, hence $[\bar{N} : N] = [\bar{F} : E]$ because of $[\bar{N} : \bar{F}] = [N : E]$.

We now want to determine the Galois group \bar{G} of $\bar{N}|\bar{F}$. Assume that we have

$$E \longleftrightarrow H.$$

Then our claim is: the Galois group \bar{G} of $\bar{N}|\bar{F}$ is isomorphic to H . We could prove this using a primitive element, but the claim has an abstract proof which is more beautiful. Since $\bar{N} \supseteq N$, every automorphism of $\bar{N}|\bar{F}$ induces an automorphism of $N|E$. In this way, \bar{G} gets mapped to a subgroup of H ; but since their orders agree, we have $\bar{G} \simeq H$. Thus our claim is proved. The two groups \bar{G} and H are related not only by this abstract isomorphism but also by the fact that applying \bar{G} to \bar{N} yields H when restricted to N . This correspondence which will be used quite often in the following will be called the *natural isomorphism* between \bar{G} and H . We have proved

Theorem 18. *If $N|F$ is Galois with Galois group G , and if \bar{F} is an arbitrary extension of F , then $\bar{N} = N\bar{F}$ is normal, and its Galois group \bar{G} is isomorphic to the subgroup H of G defined as the invariant group of the intersection*

$$E = N \cap \overline{F}.$$

Applying \overline{G} to N induces a natural map from \overline{G} to H (“natural isomorphism”).

As a consequence we emphasize that if $N|F$ is abelian, then so is $\overline{N}|\overline{F}$. Moreover we see: if K_1, K_2 are extensions of F with intersection F , and if at least one them is Galois, then

$$[K_1 K_2 : F] = [K_1 : F][K_2 : F]. \tag{1.8}$$

That the condition that one of the extensions be Galois cannot be omitted follows from the example

$$\begin{aligned} F &= \mathbb{Q} && \text{(field of rational numbers)} \\ K_1 &= \mathbb{Q}(\sqrt[3]{2}) && \text{(the real cube root of 2 is meant)} \\ K_2 &= \mathbb{Q}(\rho\sqrt[3]{2}) && (\rho \text{ is a primitive cube root of unity}), \end{aligned}$$

where $[K_1 K_2 : \mathbb{Q}] = 6$, $[K_1 : \mathbb{Q}] = [K_2 : \mathbb{Q}] = 3$.

We now can consider the intermediate fields between \overline{N} and \overline{F} . Let \overline{K} be such a field, and let \overline{U} denote the associated subgroup of \overline{G} . The group \overline{U} corresponds via the natural isomorphism to a subgroup U of G , which in turn corresponds by Galois theory to a field K . Now we claim, in analogy to the relation $E = N \cap \overline{F}$, that we have $K = N \cap \overline{K}$.

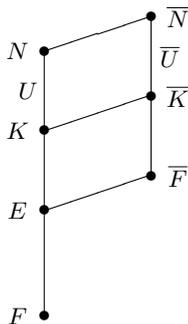


Fig. 1.3.

We first put $K_0 = N \cap E$ and have to show that $K = K_0$. Applying Theorem 18 to \overline{K} instead of \overline{F} shows that U_0 , the subgroup of G corresponding to K_0 , is isomorphic to \overline{U} , hence to U . This implies that $[N : K] = [N : K_0]$. Next K_0 , as a subfield of \overline{K} , is invariant under U , hence $K_0 \subseteq K$. Taken together this shows that $K = K_0$. We state this as

Addition (to Theorem 18). *If \overline{K} is a subextension of $\overline{N}|\overline{F}$ with associated group \overline{U} , and if K is the fixed field of the subgroup U corresponding to \overline{U} under the natural isomorphism, then*

$$K = N \cap \overline{N}.$$

Finally we want to prove a converse to Theorem 17. To this end we consider a slightly more general situation. Assume that we are given normal extensions N_1, \dots, N_s of degrees n_1, \dots, n_s over F . Assume moreover that they are independent, i.e., that we have not only $N_i \cap N_k = F$ for $i \neq k$, but even

$$N_i \cap E_i = F$$

for the composita

$$E_i = N_1 \cdots N_{i-1} \cdot N_{i+1} \cdots N_s \quad (i = 1, \dots, s).$$

Our first claim now is: the compositum $N_1 \cdots N_s = N$ is Galois. In fact, assume that $N_i = F(\theta_i)$; then

$$N = F(\theta_1, \dots, \theta_s).$$

By assumption the $\theta_i^{(\nu)}$ also lie in the N_i and generate them: we have $N_i = F(\theta_i^{(\nu_i)})$ for any ν , hence

$$N = F(\theta_1^{(\nu_1)}, \dots, \theta_s^{(\nu_s)}). \quad (1.9)$$

An arbitrary isomorphism von N sends, according to known arguments, each $\theta_i^{(\nu)}$ into some other conjugate $\theta_j^{(\kappa)}$. The representation (1.9) of N shows that this automorphism fixes N , hence $N|F$ is Galois. Since the extensions N_i are independent, a repeated applications of (1.8) shows that

$$[N : F] = \prod_i [N_i : F] = \prod_i n_i.$$

This equation allows us now to determine the Galois group of N . In fact, above we have found exactly $\prod_i n_i$ automorphisms of N , because the independence of the N_i , as is easily seen, guarantees that the ν_1, \dots, ν_s can be chosen arbitrarily, and that we get pairwise distinct automorphisms of N in this way. But since this number is just n , that is, equal to the degree of N , these are all the automorphisms of N . Each of these can be written in the form

$$\theta_1 \mapsto \theta_1^{(\nu_1)}, \dots, \theta_s \mapsto \theta_s^{(\nu_s)}.$$

(If there were any dependencies among the N_i , then the demand that $\theta_i \mapsto \theta_i^{(\nu_i)}$ could, if the ν_i are chosen freely, lead to contradictions. Consider, for example, $N_1 = \mathbb{Q}(\sqrt{2})$, $N_2 = \mathbb{Q}(\sqrt{3})$, $N_3 = \mathbb{Q}(\sqrt{6})$; then the choice $\sqrt{2} \mapsto -\sqrt{2}$, $\sqrt{3} \mapsto -\sqrt{3}$ would imply $\sqrt{6} \mapsto \sqrt{6}$, and we could not choose $\sqrt{6} \mapsto -\sqrt{6}$.)

Among the automorphisms given above there is in particular the following:

$$\theta_1 \mapsto \theta_1^{(\nu_1)}, \theta_2 \mapsto \theta_2, \dots, \theta_s \mapsto \theta_s.$$

The automorphisms of N fixing $\theta_2, \dots, \theta_s$ form a subgroup H_1 of the Galois group of N which is isomorphic to the Galois group of N_1 . Similarly we find subgroups H_i isomorphic to the Galois groups N_i . Then it is immediately seen that every automorphism of N can be written as a composition as follows:

$$\sigma = \rho_1 \cdot \rho_2 \cdots \rho_s,$$

where the ρ_i lie in the H_i and pairwise different. Every automorphism σ therefore can be represented as a *commutative* product, and this representation is unique because we can form exactly as many products in this way as there are automorphisms of N , namely $\prod_i n_i$. This shows that G is the direct product of the H_i :

$$G = H_1 \times \cdots \times H_s.$$

An additional remark about the H_i : any H_i fixes all elements of the N_k with $k \neq i$, whereas the application to N_i gives all the automorphisms of $N_i|F$. In this sense, H_i may be interpreted directly as the Galois group of N_i by demanding that an automorphism of N_i be lifted to N in such a way that the elements of all the N_k ($k \neq i$) are fixed, and that it act on all other numbers of N according to these conditions.

Thus we have proved the desired converse of Theorem 17, which we formulate as

Theorem 19. *Let N_1, \dots, N_s independent Galois extensions over F with Galois groups H_1, \dots, H_s . Then the compositum*

$$N = N_1 N_2 \cdots N_s$$

is Galois over F . If we demand that the H_j fix the elements of all N_j ($j \neq i$), then the Galois group G of $N|F$ is the direct product of the H_i :

$$G = H_1 \times \cdots \times H_s.$$

If the N_i are abelian, then so is N .

1.3 Hilbert's Theory

As an arithmetic counterpart to Galois Theory we now discuss Hilbert's Theory. Just as there the *algebraic* structure of $K|F$ is mapped into the Galois group G , here the *arithmetic* structure, i.e. the way the prime ideals \mathfrak{P} in K arise from the associated \mathfrak{p} in F , is related to G . Here of course we deal with algebraic number fields K and F of finite degree, not with abstract fields as above.

We start with the following remarks from elementary algebraic number theory: If F is an algebraic number field of finite degree and K an algebraic extension of F with finite degree n , then a prime ideal \mathfrak{p} from F has a decomposition of the form

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \quad \text{with } N\mathfrak{P}_i = \mathfrak{p}^{f_i}$$

into distinct prime ideals $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ from K , where e_i denotes the ramification index and f_i the inertia degree of \mathfrak{P}_i with respect to \mathfrak{p} . Moreover we have

$$\mathfrak{p}^n = N\mathfrak{p} = \mathfrak{p}^{e_1 f_1 + \cdots + e_g f_g} = \mathfrak{p}^{\sum e_i f_i}.$$

Comparing the exponents shows that

$$n = \sum_{i=1}^g e_i f_i.$$

Thus this equation restricts the possible decomposition types of \mathfrak{p} in K ; as a crude estimate we get

$$g \leq n, \quad e \leq n, \quad f \leq n.$$

If we specialize this decomposition law to Galois extensions $K|F$, then the prime ideals \mathfrak{P}_i all have the same ramification index e and the same inertia degree f . Thus \mathfrak{p} has the decomposition

$$\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e \quad \text{with } N\mathfrak{P}_i = \mathfrak{p}^f \text{ for } i = 1, \dots, g,$$

and we find

$$e \cdot f \cdot g = n.$$

This can be proved quickly: given a prime ideal \mathfrak{P} with $\mathfrak{P} | \mathfrak{p}$, we apply an automorphism σ of K to this relation and find

$$\mathfrak{P}^\sigma | \mathfrak{p},$$

since F and thus \mathfrak{p} are fixed under all automorphisms of $K|F$. Thus all the conjugates \mathfrak{P}^σ must also occur in the decomposition. Here \mathfrak{P}^σ of course means that σ should be applied to all elements of \mathfrak{P} ; then \mathfrak{P}^σ is a prime ideal in $K^\sigma = K$. Thus *all* conjugates of \mathfrak{P} divide \mathfrak{p} .

We show next that *only* conjugates of \mathfrak{P} divide \mathfrak{p} . Since the ideal norm is the product of conjugates, we have

$$N\mathfrak{P} = \mathfrak{p}^f = \prod_{\sigma} \mathfrak{P}^\sigma.$$

It follows that \mathfrak{p}^f is composed only from conjugate prime ideals, hence so is \mathfrak{p} :

$$\mathfrak{p} = \prod' \mathfrak{P}^\sigma,$$

where the prime indicates that the product is only over certain $\sigma \in G$. Thus we have proved that all prime ideals \mathfrak{P}_i dividing \mathfrak{p} are conjugate. Now conjugate prime ideals have the same degree and index, as follows without problems from the notion of automorphisms (from $\mathfrak{P}^e \parallel \mathfrak{p}$, i.e. $\mathfrak{P}^e | \mathfrak{p}$ but $\mathfrak{P}^{e+1} \nmid \mathfrak{p}$, we get $(\mathfrak{P}^\sigma)^e \parallel \mathfrak{p}$; and $N\mathfrak{P} = \mathfrak{p}^f$ implies $N(\mathfrak{P}^\sigma) = \mathfrak{p}^f$). Thus we have

Theorem 20. *If $K|F$ is a Galois extension, then all prime factors \mathfrak{P} of a prime ideal \mathfrak{p} from F are conjugate, and the decomposition of \mathfrak{p} into different prime ideals in K is of the following type:*

$$\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e \quad \text{with } N\mathfrak{P}_i = \mathfrak{p}^f \text{ and } efg = n.$$

Thus the last equation can also be written in the form

$$\mathfrak{p} = \left(\prod' \mathfrak{P}^\sigma \right)^e,$$

where the product is over a subset of σ in G for which the \mathfrak{P}^σ are distinct. The question of which S do occur here leads to Hilbert's theory, whose basic definitions we will give next.

Definition of the Hilbert subgroups and the associated subextensions for a given prime ideal \mathfrak{P} in K :

Definition 21. *Let \mathfrak{P} in K , \mathfrak{p} in F and n, e, f, g be defined as above, and let G be the Galois group of $K|F$.*

The set of all $\sigma \in G$ with $\mathfrak{P}^\sigma = \mathfrak{P}$ is called the decomposition group G_Z . The subfield K_Z of K associated via Galois theory to G_Z is called the decomposition field of \mathfrak{P} .

In fact, G_Z is a group, therefore a subgroup of G . This is because the only condition for subgroups of finite groups that has to be verified is, according to Theorem 9: if σ and τ fix the prime ideal \mathfrak{P} , then so does $\sigma\tau$, the composition of σ and τ .

Let σ be an arbitrary element of G_Z . If α runs through the elements of \mathfrak{P} , then α^σ runs through the elements of \mathfrak{P}^σ ; this if

$$\alpha \equiv 0 \pmod{\mathfrak{P}},$$

then

$$\alpha^\sigma \equiv 0 \pmod{\mathfrak{P}};$$

the negation also holds:

$$\alpha \not\equiv 0 \pmod{\mathfrak{P}},$$

implies

$$\alpha^\sigma \not\equiv 0 \pmod{\mathfrak{P}}.$$

Similarly, $\mathfrak{P}^a \mid \alpha$ implies $\mathfrak{P}^a \mid \alpha^\sigma$, and $\mathfrak{P}^a \nmid \alpha$ implies $\mathfrak{P}^a \nmid \alpha^\sigma$. Finally, it follows from

$$\alpha \equiv \beta \pmod{\mathfrak{P}^k}$$

that

$$\alpha^\sigma \equiv \beta^\sigma \pmod{\mathfrak{P}^k}.$$

All this implies: if α is \mathfrak{P} -integral (i.e., \mathfrak{P} does not divide the denominator of α), then so is α^σ ; if α is coprime to \mathfrak{P} , then so is α^σ .

Definition 22. *The inertia subgroup G_T of \mathfrak{P} consists of all $\sigma \in G$ that fix the individual residue classes modulo \mathfrak{P} , that is, for which*

$$\alpha^\sigma \equiv \alpha \pmod{\mathfrak{P}}$$

for every \mathfrak{P} -integral $\alpha \in K$.

The subfield K_T of K associated via Galois theory to G_T is called the inertia field of \mathfrak{P} .

Keeping in mind the consequences of Definition 21 it is easy to see that the inertia group G_T is a subgroup of G_Z . We also define

Definition 23. *The ν -th ramification G_{V_ν} of \mathfrak{P} is the set of all $\sigma \in G$ that fix every residue class modulo $\mathfrak{P}^{\nu+1}$, that is, which satisfy*

$$\alpha^\sigma \equiv \alpha \pmod{\mathfrak{P}^{\nu+1}}$$

for all \mathfrak{P} -integral $\alpha \in K$.

The subfield K_{V_ν} of K associated via Galois theory to G_{V_ν} is called the ν -th ramification field of \mathfrak{P} .

(Thus the inertia subgroup is the 0-th ramification group, so that we may occasionally write G_{V_0} for G_T and K_{V_0} for K_T .)

From the Definitions (21), (22), (23) we immediately deduce the

Theorem 24. *We have*

$$G \supseteq G_Z \supseteq G_T \supseteq G_{V_1} \supseteq \dots \supseteq 1$$

and

$$F \subseteq K_Z \subseteq K_T \subseteq K_{V_1} \subseteq \dots \subseteq K.$$

We now ask what the corresponding subgroups and subextensions are for the conjugate prime ideals \mathfrak{P}^σ . Here we have the following

Theorem 25. *The subgroup and subfield series belonging to \mathfrak{P}^σ arise by conjugation by σ from the series associated to \mathfrak{P} , i.e., are given by $\sigma^{-1}G_*\sigma$ and K_*^σ .*

Let H denote one of the subgroups of the Hilbert series associated to \mathfrak{P} . Taking e.g. the decomposition group, we see that \mathfrak{P}^σ is fixed by $\sigma^{-1}G_Z\sigma$, since

$$\mathfrak{P}^{\sigma\sigma^{-1}G_Z\sigma} = \mathfrak{P}^{G_Z\sigma},$$

and since \mathfrak{P} is fixed by G_Z , this implies

$$\mathfrak{P}^{G_Z\sigma} = \mathfrak{P}^\sigma.$$

Conversely, if

$$\mathfrak{P}^{\sigma\tau} = \mathfrak{P}^\sigma,$$

then we can deduce that

$$\mathfrak{P}^{\sigma\tau\sigma^{-1}} = \mathfrak{P},$$

i.e., $\sigma\tau\sigma^{-1} \in G_Z$, and thus $\tau \in \sigma^{-1}G_Z\sigma$. These arguments are valid analogously for the other subgroups. By the fundamental theorem of Galois theory, this implies that claim for the subfield series. Moreover we have

Theorem 26. G_T and the G_{V_i} are normal subgroups of G_Z , i.e., K_T and the K_{V_i} are normal extensions of K_Z .

Proof. Given $\sigma_\nu \in G_{V_\nu}$ and $\sigma \in G_Z$, we have to show that $\sigma^{-1}\sigma_\nu\sigma \in G_{V_\nu}$, i.e., that

$$\sigma^{-1}G_{V_\nu}\sigma = G_{V_\nu}.$$

To this end we ask how some \mathfrak{P} -integral number α behaves under the action of $\sigma^{-1}\sigma_\nu\sigma$. We have

$$\alpha^{\sigma(\sigma^{-1}\sigma_\nu\sigma)} = \alpha^{\sigma_\nu\sigma};$$

since

$$\alpha^{\sigma_\nu} \equiv \alpha \pmod{\mathfrak{P}^{\nu+1}},$$

we get

$$\alpha^{\sigma_\nu\sigma} \equiv \alpha^\sigma \pmod{(\mathfrak{P}^\sigma)^{\nu+1}},$$

hence, using $\mathfrak{P}^\sigma = \mathfrak{P}$,

$$\alpha^{\sigma_\nu\sigma} \equiv \alpha^\sigma \pmod{\mathfrak{P}^{\nu+1}}.$$

Thus we get

$$\alpha^{\sigma(\sigma^{-1}\sigma_\nu\sigma)} \equiv \alpha^\sigma \pmod{\mathfrak{P}^{\nu+1}},$$

and since α^σ runs through all \mathfrak{P} -integral numbers in K as α does, we conclude that $\sigma^{-1}\sigma_\nu\sigma \in G_{V_\nu}$, and this proves our claim. \square

It follows without problems from this theorem that G_{V_ν} is a normal subgroup of G_{V_μ} for $\mu \geq \nu$, and that K_{V_μ} is normal over K_{V_ν} .

We will now investigate how the Hilbert subgroup and subfield series behave under extension of the base field, that is, when we take a subextension E of $K|F$ as our base field. Here we have, when we denote the Galois correspondence between fields and groups by \longleftrightarrow :

Theorem 27. *If $E \longleftrightarrow H$, then we get the subgroup series for $K|E$ associated to \mathfrak{P} by taking the intersection with H of the original subgroup series; the corresponding subextensions arise by taking the compositum with E .*

Proof. We are given

$$K \subseteq E \subseteq F.$$

Let H denote the subgroup associated to E . Consider e.g. the decomposition group G'_Z of \mathfrak{P} with respect to $K|E$. Since G'_Z fixes \mathfrak{P} as well as the elements of E , we see that G'_Z is the biggest subgroup contained both in G_Z and H , and this is the intersection $G_Z \cap H$. This argument is valid analogously for the other subgroups; for the subfield series the claim follows directly from Galois theory. This proves our theorem. \square

We now want to have a closer look at the Hilbert subgroup series. But first we will give an abstract formulation of certain arguments that will occur often, so that we may refer back to it.

Let G be a group and S a set (in applications, S will be a number field, an ideal, or a residue class, and G some Galois group) on which G acts. In such a situation we ask how many $g \in G$ leave some s fixed. At first we see that the elements of G fixing s form a subgroup H of G ; all the axioms are clearly satisfied. Then if

$$G = Hg_1 + Hg_2 + \dots + Hg_j$$

is the right decomposition of G with respect to H , then two elements g, g' from the same coset (with $gg'^{-1} \in H$) act in the same way on s since

$$s^{gg'^{-1}} = g, \quad \text{hence } s^g = s^{g'}.$$

But the elements

$$s^{g_1}, s^{g_2}, \dots, s^{g_j}$$

are pairwise distinct, since it would follow from

$$s^{g_i} = s^{g_k}$$

that

$$s^{g_i g_k^{-1}} = s,$$

i.e., $g_i g_k^{-1} \in H$ and $g_i \equiv g_k \pmod{H}$. Thus the orbit of s , namely the set $\{s^g : g \in G\}$, contains exactly $j = [G : H]$ elements; all g from the same coset modulo H produce the same element. We will now apply this principle to the Galois group G and the prime ideal \mathfrak{P} in K .

Since G_Z is exactly the group of all $\sigma \in G$ that fix \mathfrak{P} , the action of G produces $[G : G_Z]$ different prime ideals. Thus the number g of different prime ideals in the decomposition

$$\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$$

satisfies the equation

$$g = [G : G_Z].$$

We also can say that, according to the above principle, the \mathfrak{P}_i correspond to the right cosets modulo G_Z , hence we can write

$$\mathfrak{P}_i = \mathfrak{P}^{G_Z \sigma_i} = \mathfrak{P}^{\sigma_i},$$

where the σ_i form a complete set of representatives of right cosets of G with respect to G_Z , so that we have:

$$G = \sum_{i=1}^g G_Z \sigma_i.$$

Thus we have determined the subset of the σ that occurred after Theorem 20:

$$\mathfrak{p} = \left(\prod_{i=1}^g \mathfrak{P}^{\sigma_i} \right)^e.$$

At the same time we find that the order of G_Z is $n/g = ef$.

These results automatically hold for the associated fields:

$$[K_Z : F] = g, \quad [K : K_Z] = ef.$$

We now want to introduce K_Z as our base field and consider not $K|F$ but $K|K_Z$. By Theorem 27 we have to form the intersection of the subgroups in the Hilbert series with the Galois group G_Z of $K|K_Z$. But since G_Z contains the groups G_Z, G_T, G_{V_1}, \dots , the Hilbert series simply becomes

$$G_Z, G_Z, G_T, G_{V_1}, \dots$$

so that only the first step has changed, and we have the same groups at the beginning. Let us first interpret the fact that the new base field K_Z is its own decomposition field with respect to \mathfrak{P} ! Letting \mathfrak{P}_Z denote the prime ideal below \mathfrak{P} in K_Z , we know from what we have proved that the degree of the decomposition field over the base field is equal to the number of different prime ideals of K dividing the prime ideal in the base field; thus we have $\mathfrak{P}_Z = \mathfrak{P}^h$. Thus in the transition from \mathfrak{P}_Z to \mathfrak{P} there occurs only ramification or an increase of the inertia degree.

Now let us investigate the ramification group. First we shall discuss the relation of G_T and G_Z . We have defined G_T as the subgroup of G whose automorphisms fix the residue classes modulo \mathfrak{P} . Now we study G_T as a subgroup of G_Z . The group G_Z does not fix the residue classes, but since $\alpha \equiv \beta \pmod{\mathfrak{P}}$ for \mathfrak{P} -integral α, β implies $\alpha^\sigma \equiv \beta^\sigma \pmod{\mathfrak{P}}$ for every $\sigma \in G_Z$, congruent numbers remain congruent under the action of the automorphisms σ , hence each residue class modulo \mathfrak{P} gets mapped to some other (possibly different) residue class. Thus the action of G_Z on the residue classes modulo \mathfrak{P} induces a *permutation* of these. Now the residue classes of K modulo \mathfrak{P} form a field¹ with $N\mathfrak{P}$ elements (where N denotes the absolute norm), and we have

$$N\mathfrak{P} = (N\mathfrak{P})^f = q^f,$$

where here and below we have put $N\mathfrak{p} = q$. If we denote the inertia degree of \mathfrak{P} with respect to \mathfrak{P}_Z by f^* and set $N\mathfrak{P}_Z = q^*$, then we can write

$$q^f = N\mathfrak{P} = (N\mathfrak{P}_Z)^{f^*} = q^{*f^*}.$$

¹ Strictly speaking, Hasse considers the ring $\mathcal{O}_{\mathfrak{P}}$ of \mathfrak{P} -integral numbers in K ; then \mathfrak{P} is a maximal ideal in $\mathcal{O}_{\mathfrak{P}}$, and its quotient $\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ is the field $K \pmod{\mathfrak{P}}$ Hasse talks about.

Certain residue classes will be fixed by G_Z , in particular those containing elements of K_Z . These residue classes may be interpreted as classes in K_Z modulo the prime ideal \mathfrak{P}_Z in K_Z below \mathfrak{P} , as the elementary theory of residue classes modulo powers of prime ideals shows. Thus the residue classes of K modulo \mathfrak{P} that form the residue class field modulo \mathfrak{P}_Z in K_Z are fixed. This shows that K modulo \mathfrak{P} is an algebraic extension of degree f^* of K_Z modulo \mathfrak{P}_Z . Our result says that G_Z induces automorphisms of $K \bmod \mathfrak{P}$ over $K_Z \bmod \mathfrak{P}_Z$. Now we claim that G_Z yields the whole Galois group of the field $K \bmod \mathfrak{P}$.

Proof. Let ρ be a primitive root mod \mathfrak{P} ; then ρ is also a primitive element for $K \bmod \mathfrak{P}$ over $K_Z \bmod \mathfrak{P}_Z$, since the powers of ρ give all elements of $K \bmod \mathfrak{P}$. Now \mathfrak{P} has degree f^* with respect to \mathfrak{P}_Z ; thus ρ satisfies a congruence

$$\varphi(\rho) \equiv 0 \pmod{\mathfrak{P}_Z}$$

which is irreducible in $K_Z \bmod \mathfrak{P}_Z$.

Moreover we know that along with ρ also $\rho^{q^*}, \rho^{q^{*2}}, \dots$ satisfy this congruence, hence are “conjugates” of ρ ; and there are f^* such conjugates. (For the q^{*f^*} -th power we have $\rho^{q^{*f^*}} \equiv \rho^{N\mathfrak{P}} \equiv \rho \pmod{\mathfrak{P}}$). These are necessarily the f^* roots of $\varphi(x)$ since $\varphi(x)$ has degree f^* . Thus $\varphi(x)$ has the decomposition

$$\varphi(x) \equiv (x - \rho)(x - \rho^{q^*}) \cdots (x - \rho^{q^{*f^*-1}}) \pmod{\mathfrak{P}_Z}.$$

□

Thus the extension $K \bmod \mathfrak{P}$ over $K_Z \bmod \mathfrak{P}_Z$ is Galois, because all its isomorphisms arise from raising the generating element ρ to the q^* -th power. *Its Galois group is cyclic* of order f^* .

Actually, the situation here is particularly simple. We claim that the automorphisms of $K \bmod \mathfrak{P}$ arise not only by raising ρ to the q^* -th, q^{*2} -th \dots power and forming the corresponding rational linear combinations; we get the automorphism by raising *each element* of $K \bmod \mathfrak{P}$ to these powers. In fact, if $\alpha \equiv \rho^a \pmod{\mathfrak{P}}$, then applying an automorphism σ mapping ρ to $\rho^{q^{*a}}$ gives

$$\alpha^\sigma \equiv (\rho^{q^*})^a \equiv (\rho^a)^{q^*} \pmod{\mathfrak{P}},$$

hence

$$\alpha^\sigma \equiv \alpha^{q^*} \pmod{\mathfrak{P}}.$$

Since the coefficients from K are fixed by Fermat’s Little Theorem for K_Z ,

$$\psi(\alpha, \beta, \dots) \equiv 0 \pmod{\mathfrak{P}}$$

implies, through exponentiating term by term,

$$\psi(\alpha^{q^*}, \beta^{q^*}, \dots) \equiv 0 \pmod{\mathfrak{P}}.$$

Thus the automorphisms of $K \bmod \mathfrak{P}$ over $K_Z \bmod \mathfrak{P}_Z$ do arise by exponentiating with $1, q^*, q^{*2}, \dots, q^{*f^*-1}$.

We now want to connect this fact with the inertia subgroup G_T . On the one hand we have considered the polynomial $\varphi(x)$; on the other hand let us investigate

$$\psi(x) = \prod_{\sigma \in G_Z} (x - \rho^\sigma) \bmod \mathfrak{P}.$$

According to by now familiar arguments (invariance of the coefficients under the action of G_Z), $\psi(x)$ is a polynomial in $K_Z \bmod \mathfrak{P}_Z$ and clearly has ρ as a root:

$$\psi(\rho) \equiv 0 \bmod \mathfrak{P}.$$

This implies that

$$\varphi(x) \mid \psi(x) \bmod \mathfrak{P}$$

since $\varphi(x)$ and $\psi(x)$ have a root in common. Thus the roots of $\varphi(x)$ all occur among the roots of $\psi(x)$; or: the conjugates of ρ with the exponents q^{*i} ($i = 0, \dots, f^* - 1$) also arise by applying automorphisms of G to ρ ; or: every automorphism of $K \bmod \mathfrak{P}$ over $K_Z \bmod \mathfrak{P}_Z$ is given by

$$\rho^{q^{*i}} \equiv \rho^{\sigma_i} \bmod \mathfrak{P},$$

where $\sigma_i \in G_Z$. This is what we have claimed.

Now $K \bmod \mathfrak{P}$ is invariant under all $\sigma \in G_T$; according to our general principle discussed above, G_Z will therefore induce exactly as many different automorphisms in the field $K \bmod \mathfrak{P}$ as there are cosets modulo G_T in G_Z , that is, we have

$$\begin{aligned} [G_Z : G_T] &= \text{number of automorphisms of} \\ &\quad K \bmod \mathfrak{P} \text{ over } K_Z \bmod \mathfrak{P}_Z, \\ f^* &= \text{order of the Galois group.} \end{aligned} \tag{1.10}$$

Conversely, the degree of the residue class field $K \bmod \mathfrak{P}$ over $K_Z \bmod \mathfrak{P}_Z$ equals $[G_Z : G_T]$.

We emphasize in particular: there is a special automorphism² Frob in G_Z which satisfies

$$\rho^{\text{Frob}} \equiv \rho^{q^*} \bmod \mathfrak{P},$$

or even for \mathfrak{P} -integral α in K :

$$\alpha^{\text{Frob}} \equiv \alpha^{q^*} \bmod \mathfrak{P}.$$

Thus among the different, algebraically completely equivalent automorphisms of $K \bmod \mathfrak{P}$ over $K_Z \bmod \mathfrak{P}_Z$ there is a unique automorphism which is arithmetically characterized by the fact that it induces exponentiating by

² This special automorphism is not called the Frobenius automorphism by Hasse.

q^{*1} . This fact will later turn out to be of fundamental importance. Moreover we see that G_Z/G_T is cyclic with Frob a representative of a generating coset. Of course every Frob^k with (k, f) will generate the factor group; but only Frob is distinguished by the property above.

We now apply our results with K_T as our base field. By Theorem 27 we get the Hilbert subgroup series for K over K_T by intersecting with G_T . Just as the first two terms in the Hilbert series with base field K_Z were equal, now the first three coincide:

$$G_T, G_T, G_T, G_V, \dots$$

According to our result (1.10) above, it follows that the inertia degree of \mathfrak{P} with respect to the prime ideal \mathfrak{P}_T in K_T below \mathfrak{P} is equal to 1, and the decomposition of \mathfrak{P}_T is of the following type:

$$\mathfrak{P}_T = \mathfrak{P}^{e^*}, \quad N_{K/K_T} \mathfrak{P} = \mathfrak{P}_T.$$

Thus the relation $efg = n$ shows

$$[G_T : 1] = [K : K_T] = e^* \cdot 1 \cdot 1 = e^*.$$

Comparing our findings now immediately leads to the desired results. It follows from

$$[G_Z : G_T] = f^*, \quad [G_T : 1] = e^*$$

that

$$[G_Z : G_T][G_T : 1] = [G_Z : 1] = e^* f^*.$$

On the other hand we have seen

$$[G_Z : 1] = ef.$$

Thus we have

$$ef = e^* \cdot f^*.$$

Now we certainly have

$$e^* \leq e, \quad f^* \leq f,$$

because f is the inertia degree and e the ramification index of \mathfrak{P} with respect to \mathfrak{p} , and these must be multiples of inertia degree and ramification index of \mathfrak{P} with respect to \mathfrak{P}_Z and \mathfrak{P}_T . Thus we must have

$$e^* = e \quad \text{and} \quad f^* = f.$$

Thus we have found rather simple results for the indices of the groups in the Hilbert series. The order of G_T is the ramification index of \mathfrak{P} , the index $[G_Z : G_T]$ is equal to the inertia degree of \mathfrak{P} . This also determines the so far unknown exponent h : we have $h = e$,

$$\mathfrak{P}_Z = \mathfrak{P}^e.$$

We find in passing that in the decomposition in K_Z

$$\mathfrak{p} = \mathfrak{P} \cdot \mathfrak{A}$$

the factor \mathfrak{A} is coprime to \mathfrak{P}_Z , since \mathfrak{A} (as an ideal in K) contains only conjugates $\mathfrak{P}^\sigma \neq \mathfrak{P}$.

We collect everything in

Theorem 28.

$$\begin{aligned} [G : G_T] = g; [G_Z : G_T] = f; \quad [G_T : 1] = e; \quad G_Z/G_T \text{ is cyclic of order } f; \\ [K_Z : F] = g; [K_T : K_Z] = f; \quad [K : K_T] = e; \quad K_T/K_Z \text{ is cyclic of order } f; \end{aligned}$$

moreover, we have:

- \mathfrak{P}_Z has inertia degree 1 and ramification index 1 with respect to \mathfrak{p} ;
- \mathfrak{P}_T has inertia degree f and ramification index 1 with respect to \mathfrak{P}_Z ;
- \mathfrak{P} has inertia degree 1 and ramification index e with respect to \mathfrak{P}_T ;
- $\mathfrak{p} = \mathfrak{P}_Z \cdot \mathfrak{A}$ with $(\mathfrak{A}, \mathfrak{P}_Z) = (1)$ in K_Z ;
- $\mathfrak{P}_Z = \mathfrak{P}_T$ in K_T ;
- $\mathfrak{P}_T = \mathfrak{P}^e$ in K .

Compare the table 1.4 on page 44.

For future reference we will state

Theorem 29. *There is an automorphism Frob in G_Z with*

$$\alpha^{\text{Frob}} \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{P}}$$

for all \mathfrak{P} -integral α in K .

Let us make a remark concerning the motivation of the expressions “decomposition field”, “inertia field”, and “ramification field”. The splitting up of a prime ideal \mathfrak{p} into pairwise distinct prime ideals in some extension field is called a “decomposition” (in the narrow sense), and we talk about “ramification” (in analogy to the situation in function fields) when the decomposition contains nontrivial powers of prime ideals. Now such a decomposition occurs when going from F to the decomposition field K_Z (compare in particular the abelian case, which will be studied below). In the transition from K_Z to K_T , the ramification index is unchanged, and there is no decomposition; in this sense the term “inertia field” is to be understood. When going from K_T to some ramification field $K_{V_1}, K_{V_2}, K_{V_3}, \dots$ there is only ramification, and the ramification index grows as large as is possible for the given field extension; we talk about “full ramification”.

Concerning the decomposition $\mathfrak{p} = \mathfrak{P}_Z \mathfrak{A}$ in K_Z we should say that, apart from \mathfrak{P}_Z , there need not exist $g - 1$ other different factors: the prime ideals

\mathfrak{P}_Z^σ belonging to the conjugates \mathfrak{P}^σ live in the conjugate fields K_Z^σ , which need not at all coincide. The Hilbert field sequence for \mathfrak{P} only explains the facts concerning \mathfrak{P} and its origin from \mathfrak{p} , but not the *complete* decomposition of \mathfrak{p} in K . The situation is different for *abelian* extensions; then the conjugate fields coincide, and in the common decomposition fields K_Z the prime ideal \mathfrak{p} has the form

$$\mathfrak{p} = \prod_{\sigma} \mathfrak{P}_Z^\sigma, \quad (\sigma \text{ system of representatives for } G/G_Z),$$

because we can argue for each conjugate prime ideal as we have done for \mathfrak{P} . This is a decomposition of \mathfrak{p} in as many different \mathfrak{P}_Z^σ as is possible for a given relative degree g ; we say that \mathfrak{p} *splits completely* in K_Z . Thus we have

Theorem 30. *If $K|F$ is abelian, then in the decomposition field \mathfrak{p} splits into g different prime ideals of inertia degree and ramification index 1 with respect to \mathfrak{p}*

$$\mathfrak{p} = \prod_i \mathfrak{P}_Z^{\sigma_i},$$

where

$$G = \sum_{i=1}^g G_Z \sigma_i.$$

Let us now characterize decomposition fields and inertia fields in a way that differs from that given in Definitions 22 and 23. In fact we want to show that our results imply certain maximality properties of decomposition and ramification fields.

We want to prove:

- a) K_Z is the maximal subextension of $K|F$ in which the prime ideal below \mathfrak{P} has inertia degree 1 and ramification index 1 with respect to \mathfrak{p} .
- b) K_T is the maximal subextension of $K|F$ in which the prime ideal below \mathfrak{P} has ramification index 1 with respect to \mathfrak{p} .

Let us assume that a) E is a subextension of $K|F$ associated to the Galois group H in which the prime ideal \mathfrak{P}_E below \mathfrak{P} has inertia degree and ramification index 1 with respect to \mathfrak{p} , and that b) E' is subextension of $K|F$ associated to the Galois group H' in which the prime ideal $\mathfrak{P}_{E'}$ below \mathfrak{P} has ramification index 1 with respect to \mathfrak{p} . Then our claim reads

$$E \subseteq K_Z, \quad E' \subseteq K_T.$$

Thus according to our assumptions, multiplicativity of inertia degree and ramification index show that \mathfrak{P} has degree f and index e with respect to \mathfrak{P}_E . Similarly, \mathfrak{P} has order e with respect to E' . Now we take E and E' as

our base fields, respectively, and form the groups \overline{G}_Z and \overline{G}'_T belonging to \mathfrak{P} over these fields. The observations that we just made imply:

$$\begin{aligned} [\overline{G}_Z : 1] &= ef = [G_Z : 1]; \\ [\overline{G}'_T : 1] &= f = [G_T : 1]. \end{aligned}$$

On the other hand, according to our general theorems on the behavior of Hilbert groups under base change we have

$$\begin{aligned} \overline{G}_Z &= G_Z \cap H, \quad \text{hence } \overline{G}_Z \subseteq G_Z, \\ \overline{G}'_T &= G_T \cap H, \quad \text{hence } \overline{G}'_T \subseteq G_T. \end{aligned}$$

Together with the equations concerning the order we get

$$\begin{aligned} \overline{G}_Z &= G_Z, \\ \overline{G}'_T &= G_T, \end{aligned}$$

hence

$$\begin{aligned} G_Z &\subseteq H, \quad \text{i.e., } K_Z \subseteq E, \\ G_T &\subseteq H', \quad \text{i.e., } K_T \subseteq E. \end{aligned}$$

Thus we have proved:

Theorem 31 (Maximality of Decomposition and Inertia Field).

- a) K_Z is the maximal subextension of $K|F$ for which the prime ideal below \mathfrak{P} has inertia degree and ramification index 1 with respect to \mathfrak{p} .
- b) K_T is the maximal subextension of $K|F$ for which the prime ideal below \mathfrak{P} has ramification index 1 with respect to \mathfrak{p} .

We now want to consider this theorem in the special case where $K|F$ is abelian: then the Hilbert field and group series for the different prime factors \mathfrak{P}^σ of \mathfrak{p} in K , which in general are conjugate fields and groups, coincide because we are dealing with *abelian* groups, in which all subgroups are normal. In particular, all \mathfrak{P}^σ share the same decomposition field K_Z and the same inertia field K_T . Thus we can add the following complement to Theorem 31:

Addition (to Theorem 31):

For abelian extensions,

- a) K_Z is the maximal subextension of $K|F$ in which \mathfrak{p} splits completely (i.e. splits into distinct prime ideals of inertia degree and ramification index 1).
- b) K_T is the maximal subextension of $K|F$ in which \mathfrak{p} is unramified (i.e. splits into distinct prime ideals of inertia degree 1).

We next look at the ramification fields. First we are interested in the question whether this series can be infinitely long, say because from some point on all G_{V_i} coincide, or whether the series terminates because eventually $G_{V_i} = 1$. The fact that the latter possibility always holds can be seen as follows: let θ be an \mathfrak{P} -integral primitive element for $K|F$; then the θ^σ are pairwise distinct. For σ to belong to G_{V_i} we must have $\mathfrak{P}^{i+1} \mid (\theta - \theta^\sigma)$. Since each such difference is divisible by at most a fixed power of \mathfrak{P} as soon as $\theta \neq \theta^\sigma$, i.e., $\sigma \neq 1$, for some index i on we must have $G_{V_i} = 1$. If there is ramification above \mathfrak{p} and if $G_{V_v} \neq 1$ but $G_{V_{v+1}} = 1$, then v is called the *ramification number*; in the case $v = 0$ we say there is no higher ramification. We observe:

Theorem 32. *For every Galois extension $K|F$ there exists an integer v such that $G_{V_i} = 1$ for all $i > v$.*

Now let π be a uniformizer for \mathfrak{P} , that is, $\mathfrak{P} \parallel \pi$. Then every $\sigma \in G_{V_i}$ ($i \geq 0$) satisfies the congruence

$$\pi^\sigma \equiv \pi \pmod{\mathfrak{P}^{i+1}}.$$

Conversely, if σ is an automorphism in G_T for which this congruence holds, then it is easy to verify that σ must belong to G_{V_i} . In fact, every \mathfrak{P} -integral α can be written in the form

$$\alpha = x_0 + x_1\pi + \dots + x_i\pi^i \pmod{\mathfrak{P}^i},$$

where the x_i are from a fixed system of residues modulo \mathfrak{P} . Since \mathfrak{P}_T has the same inertia degree as \mathfrak{P} , we can choose this system of residues in K_T . Then applying σ gives

$$\begin{aligned} \alpha^\sigma &\equiv x_0 + x_1\pi^\sigma + \dots + x_i(\pi^i)^\sigma \\ &\equiv x_0 + x_1\pi + \dots + x_i\pi^i \equiv \alpha \pmod{\mathfrak{P}^{i+1}}, \end{aligned}$$

and this means that $\sigma \in G_{V_i}$. Thus G_{V_i} consists of those and only those automorphisms $\sigma \in G_T$ for which $\pi^\sigma \equiv \pi \pmod{\mathfrak{P}^i + 1}$; this characterization of G_{V_i} will now be exploited.

If σ is an element of G_T , then π^σ must be divisible exactly once by \mathfrak{P} , hence

$$\pi^\sigma \equiv x_\sigma \pi \pmod{\mathfrak{P}^2}$$

for some x_σ defined modulo \mathfrak{P} , and which therefore can be chosen from K_T . There is such a coprime residue class $x_\sigma \pmod{\mathfrak{P}}$ associated to every $\sigma \in G_T$. If x_τ is associated in this sense to some other element $\tau \in G_T$, then applying τ yields

$$\pi^{\sigma\tau} = (\pi^\sigma)^\tau \equiv (x_\sigma \pi)^\tau \equiv x_\sigma^\tau \pi^\tau \equiv x_\sigma (x_\tau \pi) \equiv (x_\sigma x_\tau) \pi \pmod{\mathfrak{P}^2}.$$

Thus the residue class associated to $\sigma\tau$ is $x_\sigma x_\tau \bmod \mathfrak{P}$. Under this map sending σ to x_σ those and only those σ correspond to the unit element for which

$$\pi^\sigma \equiv 1 \cdot \pi \bmod \mathfrak{P}^2,$$

that is, those that, according to our introductory remark, belong to G_V . According to well known and often used arguments the factor group G_T/G_V is thus isomorphic to the group of these coprime residue classes modulo \mathfrak{P} , i.e., to a subgroup of order $N\mathfrak{P} - 1$ of the coprime residue class group modulo \mathfrak{P} . If we denote the order of the factor group G_T/G_V by e_0 , then e_0 divides $N\mathfrak{P} - 1$, and hence is coprime to p . As a subgroup of a cyclic group, this factor group is also *cyclic*. We formulate this result:

Theorem 33. G_T/G_V is cyclic of order e_0 coprime to p . Here $e_0 \mid N\mathfrak{P} - 1$ and $e = e_0 p^r$; thus e_0 is the part of e coprime to p .

The last assertion of this theorem will be seen to be correct right after Theorem 34.

The elements of G_{V_i} are characterized as those elements of G_T for which $\pi^\sigma \equiv \pi \bmod \mathfrak{P}^{i+1}$. Thus

$$\pi^\sigma \equiv \pi + y_\sigma \pi^{i+1} \bmod \mathfrak{P}^{i+2}$$

for some element y_σ that is defined modulo \mathfrak{P} and can be chosen from K_T . Thus to each element of G_V we can associate a residue class modulo \mathfrak{P} which is, however, not necessarily coprime to \mathfrak{P} . Again we ask which residue class corresponds to the product $\sigma\tau$ of two automorphisms $\sigma, \tau \in G_T$. Applying τ yields

$$\begin{aligned} \pi^{\sigma\tau} &\equiv (\pi + y_\sigma \pi^{i+1})^\tau \equiv \pi^\tau + y_\sigma (\pi^\tau)^{i+1} \\ &\equiv \pi^\tau + y_\sigma (\pi + y_\tau \pi^{i+1})^{i+1} \\ &\equiv \pi + (y_\sigma + y_\tau) \pi^{i+1} \bmod \mathfrak{P}^{i+2}; \end{aligned}$$

thus $y_{\sigma\tau} \equiv y_\sigma + y_\tau \bmod \mathfrak{P}^{i+2}$. For those and only those $\sigma \in G_{V_i}$ that are also in $G_{V_{i+1}}$ we have

$$\pi^\sigma \equiv \pi + 0 \cdot \pi^{i+1} \equiv \pi \bmod \mathfrak{P}^{i+2}.$$

Thus for exactly these σ we have $y_\sigma \equiv 0 \bmod \mathfrak{P}$. According to the same principle as above $G_{V_i}/G_{V_{i+1}}$ is isomorphic to some subgroup of the additive group of residue classes modulo \mathfrak{P} . This last group has type (p, p, \dots, p) , since $p\alpha \equiv 0 \bmod \mathfrak{P}$, and the order of this group is equal to $N\mathfrak{P}$; thus every subgroup has this type and an order dividing $N\mathfrak{P}$. We have proved:

Theorem 34. $G_{V_i}/G_{V_{i+1}}$ is abelian of type (p, p, \dots, p) , and has order at most $N\mathfrak{P}$ ($i \geq 1$).

The last remark gives an upper bound for the orders of the factor groups $G_{V_i}/G_{V_{i+1}}$, about which we cannot say much more in general. Since the sequence of the G_{V_i} terminates after finitely many steps, the orders of the G_{V_i} , in particular the order of $G_{V_1} = G_V$, are products of the orders of the factor groups, and thus are prime powers p^{r_i} . Since in particular we must have $e = e_0 p^{r_1}$, the last claim in Theorem 33 is now proved. Moreover we now can determine the prime ideals \mathfrak{P}_{V_i} below \mathfrak{P} in the K_{V_i} . Since \mathfrak{P}_T , as was already proved, ramifies completely in K , the same must be true for the intermediate fields between K and K_T , hence

$$\mathfrak{P}_T = \mathfrak{P}_V^{e_0} \quad \text{and} \quad \mathfrak{P}_{V_i} = \mathfrak{P}_{V_{i+1}}^{p^{r_i - r_{i+1}}}; \quad \text{moreover } \mathfrak{P}_{V_i} = \mathfrak{P}^{p^{r_i}}.$$

Compare these relations with Table 1.4 on page 44. Now we can, just as we did before for the decomposition field and the inertia field, prove a maximality property for the field K_V called the ramification field, which plays a distinguished role among the following “higher” ramification fields. We have:

Theorem 35. *K_V is the maximal subextension of $K|F$ in which the ramification index of the prime ideal below \mathfrak{P} with respect to \mathfrak{p} is coprime to p .*

The proof is also completely analogous to what we did earlier. In fact, let E be a subextension of $K|F$ with the above properties, and let H be the subgroup corresponding to E via Galois theory. The ramification subgroup for \mathfrak{P} with E as our base field has order at least p^{r_1} , since this is the ramification index of \mathfrak{P} over K_V . On the other hand, by Theorem 25 it equals the intersection $H \cap G_V$. Since G_V already has order p^{r_1} , we have $H \supseteq G_V$, and this is what we wanted to prove.

Hilbert’s theory also provides us with an exact determination of the different and the discriminant of Galois fields. We only want to carry this out for the different as defined in Kronecker’s theory, which is more convenient for this purpose, and will not discuss the proof that this notion is equivalent to that given by Dedekind. In fact, if σ is a nontrivial automorphism of the Galois group G of $K|F$, then according to Hilbert the greatest common divisor of all numbers $\alpha - \alpha^\sigma$, formed with all integers α , is called the element \mathfrak{E}_σ associated to σ . Then the definition of the relative different is

$$\text{diff}(K|F) = \prod_{\sigma \neq 1} \mathfrak{E}_\sigma,$$

where the product is over all $\sigma \neq 1$ in G . It is this definition due to Kronecker that we will now work with.

Using this definition it is easy to determine the contribution $\text{diff}_{\mathfrak{P}}(K|F)$ of \mathfrak{P} to $\text{diff}(K|F)$. According to the defining congruence relations for the G_{V_i} , the prime ideal \mathfrak{P} contributes, if σ is in G_{V_i} , but not in $G_{V_{i+1}}$ (that is, if $\sigma \in G_{V_i} \setminus G_{V_{i+1}}$, as we will write), the factor $\mathfrak{E}_\sigma(\mathfrak{P}) = \mathfrak{P}^{i+1}$ to \mathfrak{E}_σ . This holds

for $i = 0, 1, 2, \dots$ if we put $G_{V_0} = G_T$. The σ not in G_T do not contribute any \mathfrak{P} -factor to $\text{diff}(K|F)$. Since $G_{V_0} \setminus G_{V_1}$ contains exactly $e - p^{r_1}$ elements, and $G_{V_i} \setminus G_{V_{i+1}}$ exactly $p^{r_i} - p^{r_{i+1}}$ elements (compare Table 1.4 on page 44), we find:

$$\begin{aligned} \text{diff}_{\mathfrak{P}} &= \mathfrak{P}^{(e-p^{r_1})+2(p^{r_1-r_2})+\dots+(v+1)(p^{r_v}-1)} \\ &= \mathfrak{P}^{e+\sum_{i=1}^v p^{r_i}-(v+1)}. \end{aligned}$$

Collecting terms differently, first the contribution \mathfrak{P} for all $\sigma \neq 1$ in G_T , then that for the $\sigma \neq 1$ in G_{V_1} etc., then we get

$$\text{diff}_{\mathfrak{P}} = \mathfrak{P}^{e-1+\sum_{i=1}^v (p^{r_i}-1)}.$$

For the discriminant we get, since $\text{disc}(K|F) = N \text{diff}(K|F) = \text{diff}(K|F)^n$,

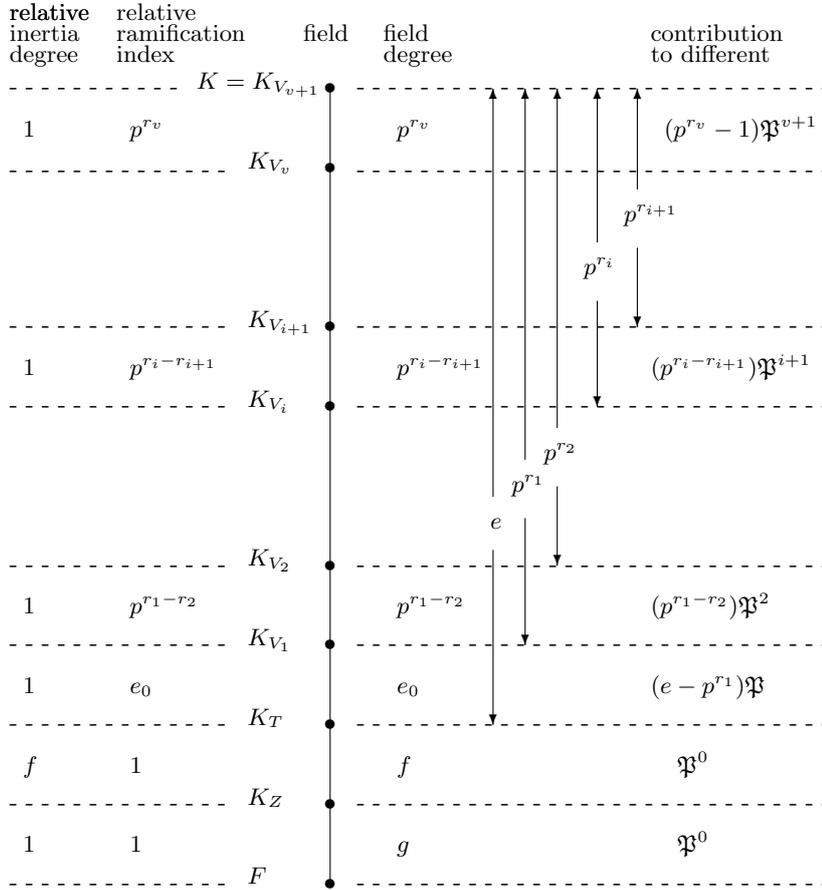
$$\text{disc}_{\mathfrak{P}} = \mathfrak{P}^{n[e-1+\sum_{i=1}^v (p^{r_i}-1)]},$$

or, since $\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$,

$$\text{disc}_{\mathfrak{p}}(K|F) = \mathfrak{p}^{fg[e-1+\sum_{i=1}^v (p^{r_i}-1)]}.$$

In the first term $e - 1$ inside the bracket we recognize the number occurring in Dedekind's discriminant theorem; for Galois extensions, this formula complements Dedekind's theorem in a completely satisfactory way.

Fig. 1.4. The Prime Ideals below \mathfrak{P}



With this figure we will for now leave Hilbert's theory proper. However, let us briefly discuss the relations to Hilbert's theory for extensions of the \mathfrak{p} -adic numbers. These relations have turned out to be extremely important, and are of particular relevance for class field theory.

Thus let K be an arbitrary (finite) Galois extension of F and \mathfrak{P} a prime ideal from K . Then we extend K to Hensel's completion $K_{\mathfrak{P}}$ of \mathfrak{P} -adic numbers by completing \mathfrak{P} with respect to the valuation induced by \mathfrak{P} in the well known way. The valuation by \mathfrak{P} restricts to the valuation induced by \mathfrak{p} (or an equivalent valuation) on F , hence the completion $K_{\mathfrak{P}}$ also contains the completion of F with respect to \mathfrak{p} ; this means that $K_{\mathfrak{P}}$ contains the field $F_{\mathfrak{p}}$. Thus $K_{\mathfrak{P}}$ contains both K and $F_{\mathfrak{p}}$, and we can form the compositum $K \cdot F_{\mathfrak{p}}$. Our first claim is that

$$K_{\mathfrak{P}} = K \cdot F_{\mathfrak{p}}.$$

We will prove our claim in two steps, and we start by observing that $K \cdot F_{\mathfrak{p}}$ is contained in $K_{\mathfrak{P}}$. This is clear according to what we already said, since both factors are contained in $K_{\mathfrak{P}}$. Now we show conversely that $K_{\mathfrak{P}}$ is contained in $K \cdot F_{\mathfrak{p}}$. To this end we have to study the structure of $K_{\mathfrak{P}}$ more closely.

Let $\mathfrak{P} \parallel \Pi$, i.e., let $\Pi \in K$ be a number divisible by \mathfrak{P} and not by \mathfrak{P}^2 ; similarly pick some number $\pi \in K$ with $\mathfrak{p} \parallel \pi$. Then the numbers in $K_{\mathfrak{P}}$ have the representation

$$\sum_{\nu=\nu_0}^{\infty} \gamma_{\nu} \Pi^{\nu}.$$

But instead of using the powers of Π for developing numbers, we can also make use of the element π since the only thing that matters is the power of Π dividing the element. If \mathfrak{P} has ramification index e with respect to \mathfrak{p} , then $\mathfrak{P}^e \parallel \mathfrak{p}$, and we can use the sequence

$$1, \Pi, \Pi^2, \dots, \Pi^{e-1}, \pi, \pi \Pi, \dots, \pi \Pi^{e-1}, \pi^2, \dots$$

instead of the powers of Π . Thus we arrive at a representation of an arbitrary number in $K_{\mathfrak{P}}$ in the form

$$\alpha = \sum_{k=0}^{e-1} \sum_{l=l_0}^{\infty} \gamma_{kl} \Pi^k \pi^l,$$

where the γ_{kl} are taken from certain residue classes modulo \mathfrak{P} . Since the number of residue classes does not change under the extension from K to $K_{\mathfrak{P}}$, we can choose the γ_{kl} from this residue system in K . Now let $1, \theta, \dots, \theta^{n-1}$ be a basis of $K|F$ and

$$\gamma_{kl} = \sum_{\nu=0}^{n-1} c_{kl\nu} \theta^{\nu} \quad \text{with } c_{kl\nu} \in F.$$

Then

$$\alpha = \sum_{l=l_0}^{\infty} \sum_{k=0}^{e-1} \sum_{\nu=0}^{n-1} c_{kl\nu} \theta^{\nu} \Pi^k \pi^l = \sum_{k=0}^{e-1} \sum_{\nu=0}^{n-1} \left[\sum_{l=l_0}^{\infty} c_{kl\nu} \pi^l \right] \theta^{\nu} \Pi^k.$$

Now this is a representation of α by θ, Π , and numbers in F ; it shows directly that $K_{\mathfrak{P}}$ indeed can be composed from $F_{\mathfrak{p}}$ and K , i.e.

$$K_{\mathfrak{P}} \subseteq K \cdot F_{\mathfrak{p}}.$$

Thus we have proved that

$$K_{\mathfrak{P}} = K \cdot F_{\mathfrak{p}}.$$

At this point we would like to include a warning as to how not to prove this result. Above we have first constructed $K_{\mathfrak{P}}$, then formed the compositum

$K \cdot F_{\mathfrak{p}}$ out of the two subfields K and $F_{\mathfrak{p}}$, and then proved the equality $K_{\mathfrak{P}} = K \cdot F_{\mathfrak{p}}$. Now one could try the following idea: Let K be a given Galois extension of F and \mathfrak{p} a prime ideal in F . Take the completion $F_{\mathfrak{p}}$ and form the compositum $K \cdot F_{\mathfrak{p}}$. Is this equal to the field $K_{\mathfrak{P}}$? This is hardly possible, since $K_{\mathfrak{P}}$ depends on the choice of the prime ideal \mathfrak{P} among its conjugates $\mathfrak{P}', \mathfrak{P}'', \dots$ (there exist numbers divisible by \mathfrak{P} and not by \mathfrak{P}'), whereas the construction $K \cdot F_{\mathfrak{p}}$ does not take the difference between \mathfrak{P} and its conjugates into account. In fact we readily see that the compositum $K \cdot F_{\mathfrak{p}}$ is not even well defined: it is not at all clear what the sum of an element of K and an element of $F_{\mathfrak{p}}$ (which do not both belong to F) should be. One could however try and *define* this composition as follows: let $K = F(\theta)$. Then K consists of all expressions

$$c_0 + c_1\theta + \dots + c_{n-1}\theta^{n-1}$$

with coefficients $c_i \in F$. We may say that K consists of all polynomials $g(\theta)$. Here polynomials of degree n and higher have to be reduced to polynomials of degree less than n by using the equation $f(\theta) = 0$ of degree n for θ in F . In other words: K is isomorphic to the residue class field of all polynomials $g(x)$ modulo $f(x)$. It is easy to see that the residue class ring of all polynomials $g(x)$ modulo some *irreducible* polynomial $f(x)$ *always* is a field. In an analogous way we now could define: we work with all expressions

$$\bar{c}_0 + \bar{c}_1\theta + \dots + \bar{c}_{n-1}\theta^{n-1},$$

where the \bar{c}_i are elements of $F_{\mathfrak{p}}$. As soon as we get polynomials of degree $> n - 1$, we reduce them using the equation $f(\theta) = 0$ to an expression of the form above. This is indeed a possible definition, as can be seen best using the second interpretation discussed above. Thus we would get the residue class ring modulo $f(x)$ of all polynomials $g(x)$ with coefficients in $F_{\mathfrak{p}}$. In general, however, the irreducible polynomial $f(x)$ in F will become reducible in $F_{\mathfrak{p}}$, and have the decomposition

$$f(x) = \bar{f}_1(x) \cdots \bar{f}_r(x)$$

into irreducible factors in $F_{\mathfrak{p}}$. Then according to our definition we have $f(\theta) = 0$, but $\bar{f}_1(\theta) \neq 0, \dots, \bar{f}_r(\theta) \neq 0$, since these factors all have degree less than n . Thus a product would be zero without some factor being zero; there exist proper zero divisors. This is impossible in a field. Therefore our ring defined above is not a field, but is subsumed under more general notions studied in the theory of algebras and which here are not of interest to us. Thus this definition of a compositum $K \cdot F_{\mathfrak{p}}$ fails. – We now could consider the residue class ring with respect to one of the irreducible factors $\bar{f}_i(x)$. Then one indeed gets fields, but of course they will depend on the choice of the irreducible polynomials $\bar{f}_i(x)$. It can be seen without difficulty that this ambiguity is connected with the different $\mathfrak{P}_i \mid \mathfrak{p}$, and that this construction gives, up to isomorphisms, exactly the different fields $K_{\mathfrak{P}_i}$. We do not want

to follow up on this idea, however. We only want to emphasize again that in *our* construction the compositum $K \cdot F_{\mathfrak{p}}$ was defined *within* $K_{\mathfrak{P}}$, that is, *after* the construction of $K_{\mathfrak{P}}$. Although this is not clear from the notation, $K \cdot F_{\mathfrak{p}}$ depends on \mathfrak{P} , that is, on the choice of the prime factor \mathfrak{P}_i of \mathfrak{p} that is used for the completion $K_{\mathfrak{P}}$.

After this intermission we return to our actual topic. The four fields F , $F_{\mathfrak{p}}$, K and $K_{\mathfrak{P}}$ are connected in a way we have often seen before and which is displayed in Figure 1.5. Since $K|F$ is Galois, then according to our earlier investigations so is $K_{\mathfrak{P}}|F_{\mathfrak{p}}$, and its Galois group is isomorphic to the invariant group belonging to the intersection

$$E = K \cap F_{\mathfrak{p}};$$

these two groups are actually equal if we identify (via a canonical isomorphism) an automorphism of $K_{\mathfrak{P}}|F_{\mathfrak{p}}$ with the automorphism of $K|F$ it induces. Determining the group $G_{\mathfrak{p}}$ of $K_{\mathfrak{P}}|F_{\mathfrak{p}}$ thus boils down to determining $E = K \cap F_{\mathfrak{p}}$ and its invariant group. This is what we will do first.

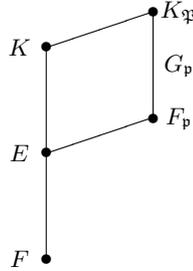


Fig. 1.5.

We know that the elements of $F_{\mathfrak{p}}$ can be written in the form

$$\alpha = c_a \pi^a + c_{a+1} \pi^{a+1} + \dots,$$

where π is an element of F which is exactly divisible by \mathfrak{p} , and where the c_i are taken from a fixed residue system modulo \mathfrak{p} in F . In particular, such a representation exists for the numbers of E . For the \mathfrak{p} -integral numbers we have $a \geq 0$, and the integer a gives the exact power of π (or \mathfrak{p}) that divides α . Thus every integral α is either coprime to \mathfrak{p} ($a = 0$) or divisible by an *integral* power \mathfrak{p}^a ($a > 0$) of \mathfrak{p} . If \mathfrak{Q} is the prime ideal below \mathfrak{P} in E , then a number of E divisible exactly by \mathfrak{Q} (which cannot be coprime to \mathfrak{p}) must be divisible at least once, and therefore exactly once, by π (or \mathfrak{p}). But this means that the numbers divisible exactly once by \mathfrak{Q} coincide with those exactly divisible by \mathfrak{p} , i.e. \mathfrak{Q} divides \mathfrak{p} exactly once, and \mathfrak{Q} has ramification index 1 with respect to \mathfrak{p} (\mathfrak{p} is unramified in $E|F$). Now the given representation shows moreover that the c_i form a complete system of residues modulo \mathfrak{Q} . Thus the number

of residue classes did not increase from \mathfrak{p} to Ω , hence Ω has inertia degree 1 with respect to \mathfrak{p} .

These two remarks imply, according to Theorem 31 on the maximality property of the decomposition field K_Z of \mathfrak{P} , that the field E must be a subfield of K_Z . Conversely it is immediately seen that K_Z is contained in $F_{\mathfrak{p}}$, hence in E . In fact, since \mathfrak{P}_Z has ramification index 1 with respect to \mathfrak{p} , any number divisible exactly once by \mathfrak{P}_Z is also divisible exactly once by \mathfrak{p} ; let π be such a number in F . Moreover we can choose a complete residue system mod \mathfrak{P}_Z in F . If α is an arbitrary number in K_Z , then we can find an infinite sequence c_0, c_1, c_2, \dots of numbers from this residue system such that

$$\alpha \equiv c_0 + c_1\pi + \dots + c_k\pi^k \pmod{\mathfrak{P}_Z^{k+1}}$$

for all $k \geq 0$. In the \mathfrak{p} -adic language this says that α can be developed into a \mathfrak{p} -adic series, and therefore lies in $F_{\mathfrak{p}}$. – Thus we have proved that $E = K_Z$. This is an extremely important result: constructing $K_{\mathfrak{P}}$ as a compositum of K with $F_{\mathfrak{p}}$ means adjoining exactly the numbers of the decomposition field K_Z .

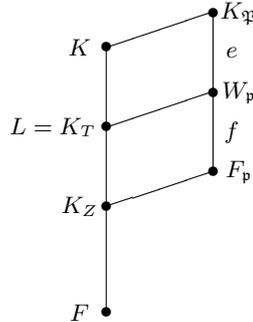


Fig. 1.6.

It is now possible to get a closer relation between Hensel’s and Hilbert’s theories. In Hensel’s theory it is known that there is a uniquely determined subextension $W_{\mathfrak{p}}$ of $K_{\mathfrak{P}}|F_{\mathfrak{p}}$ of degree f over $F_{\mathfrak{p}}$ called Hensel’s “coefficient field”, which is unramified over $F_{\mathfrak{p}}$ and whose elements therefore admit developments into powers of π , but in which the new residue class field has degree f over the old one. The field $W_{\mathfrak{p}}$ corresponds to a subfield L of K whose invariant group is the same as (or, under the natural isomorphism, corresponds to) that of $W_{\mathfrak{p}}$, and which according to the Addition to Theorem 18 is equal to the intersection $W_{\mathfrak{p}} \cap K$. This last representation of L shows that L is a subfield of $W_{\mathfrak{p}}$, hence we can argue exactly as above for $F_{\mathfrak{p}}$ and find that the prime ideal \mathfrak{P}_L of L is *unramified*, that is, has ramification index 1. According to the maximality property of the inertia field (Theorem 31) this

implies that $L \subseteq K_T$, and since both fields have degree f over K , we find $L = K \cap W_{\mathfrak{p}} = K_T$ (in particular $\mathfrak{P}_L = \mathfrak{P}_T$).

Finally let us mention that $F_{\mathfrak{p}}$ is the \mathfrak{P}_Z -adic completion of K_Z , since this follows without problems from the development into series or via arguments involving valuations ($F_{\mathfrak{p}}$ is a complete extension of K_Z). Similarly we have $W_{\mathfrak{p}} = (K_T)_{\mathfrak{P}_T}$, the \mathfrak{P}_T -adic completion of K_T , for the same reasons.

It is, by the way, possible to proceed in the inverse direction by constructing the field \overline{K}_T as the \mathfrak{P}_T -adic completion of the inertia field and then proving that it has the properties of $W_{\mathfrak{p}}$, showing in this way also the existence of such a $W_{\mathfrak{p}}$.

We formulate these results as follows:

Theorem 36. *For the \mathfrak{P} -adic completion $K_{\mathfrak{P}}$ and the associated \mathfrak{p} -adic completion $F_{\mathfrak{p}}$ we have, within $K_{\mathfrak{P}}$:*

$$K_{\mathfrak{P}} = K \cdot F_{\mathfrak{p}}, \quad K_Z = K \cap F_{\mathfrak{p}}.$$

The Galois group of $K_{\mathfrak{P}}|F_{\mathfrak{p}}$ is therefore isomorphic to the decomposition group G_Z , and fixed field of the inertia group G_T is the coefficient field $W_{\mathfrak{p}}$, i.e., $K_T = K \cap W_{\mathfrak{p}}$. Moreover we have

$$F_{\mathfrak{p}} = (K_Z)_{\mathfrak{P}_Z}, \quad W_{\mathfrak{p}} = (K_T)_{\mathfrak{P}_T}$$

for the prime ideals \mathfrak{P}_Z in K_Z and \mathfrak{P}_T in K_T below \mathfrak{P} .

1.4 The Artin Symbol

In this section we want to deduce from Hilbert's ramification theory a few consequences that will be very important in the following. To this end we consider, for a number field F , an arbitrary Galois extension $K|F$ which, at first, is not necessarily Abelian. Let \mathfrak{P} be a prime ideal in K not dividing the different $\text{diff}(K|F)$, that is, a prime ideal in K unramified in $K|F$. Then the inertia group G_T of \mathfrak{P} is the trivial group since the ramification index of \mathfrak{P} equals 1. Moreover, $K = K_T$ is its own inertia field, hence $K|K_Z$ is a cyclic extension of degree f , the inertia degree of \mathfrak{P} over F . Then the cyclic group G_Z of order f has $\varphi(f)$ generators, among which there is, as we have remarked explicitly in the last section, a distinguished automorphism Frob , namely the one that satisfies

$$\alpha^{\text{Frob}} \equiv \alpha^{N_{\mathfrak{p}}} \pmod{\mathfrak{P}} \tag{1.11}$$

for all \mathfrak{P} -integral $\alpha \in K$. This congruence uniquely determines the automorphism Frob as an element of G_Z : if $\alpha^{\sigma} \equiv \alpha^{N_{\mathfrak{p}}}$, then

$$\alpha^{\text{Frob}} \equiv \alpha^{\sigma}, \alpha^{\text{Frob} \sigma^{-1}} \equiv \alpha \pmod{\mathfrak{P}},$$

hence $\text{Frob} \sigma^{-1}$ fixes all residue classes modulo \mathfrak{P} , and therefore $\text{Frob} \sigma^{-1} \in G_T$; since $G_T = 1$, we have $\text{Frob} \sigma^{-1} = 1$ and $\text{Frob} = \sigma$. We define

Definition 37. If $\mathfrak{P} \nmid \text{diff}(K|F)$, hence if $G_T = 1$ and G_Z is cyclic of order f , then the generator Frob of G_Z uniquely determined by \mathfrak{P} and (1.11) is called the *Frobenius automorphism of \mathfrak{P} with respect to $K|F$* ; it is denoted by

$$\text{Frob} = \left[\frac{K}{\mathfrak{P}} \right] = \left[\frac{K|F}{\mathfrak{P}} \right] \quad (\text{Frobenius Symbol}).$$

Applying an arbitrary automorphism $\sigma \in G$ to (1.11) we get

$$\alpha^{\text{Frob} \sigma} \equiv (\alpha^\sigma)^{N\mathfrak{p}} \pmod{\mathfrak{P}^\sigma} \quad \text{for all } \mathfrak{P}\text{-integral } \alpha \in K.$$

As α runs through all \mathfrak{P} -integral numbers, α^σ runs through all \mathfrak{P}^σ -integral numbers; since $\alpha' = \alpha^\sigma$ implies $\alpha = \alpha'^{\sigma^{-1}}$, we find

$$\alpha'^{\sigma^{-1}\text{Frob} \sigma} \equiv \alpha'^{N\mathfrak{p}} \pmod{\mathfrak{P}^\sigma}$$

for all \mathfrak{P}^σ -integral α' . Since this congruence determines the Frobenius automorphism, we find that the Frobenius automorphism of \mathfrak{P}^σ is $\sigma^{-1}\text{Frob} \sigma$:

Theorem 38.

$$\left[\frac{K}{\mathfrak{P}^\sigma} \right] = \sigma^{-1} \left[\frac{K}{\mathfrak{P}} \right] \sigma.$$

We now specialize this result to the case which is particularly important for us, namely when K is abelian over F . Then by Theorem 38 the congruence (1.11) holds for all conjugate prime ideals \mathfrak{P}^σ with *the same* automorphism Frob ; hence it is valid, since $\mathfrak{p} = \prod_\sigma \mathfrak{P}^\sigma$ (the product being over all different \mathfrak{P}^σ) is unramified in K , modulo \mathfrak{p} :

$$\alpha^{\text{Frob}} \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{p}} \tag{1.12}$$

for all \mathfrak{p} -integral α . Thus in this case Frob *only depends on \mathfrak{p}* . The defining condition for this symbol now reads, formulated with \mathfrak{p} : $\mathfrak{p} \nmid \text{disc}(K|F)$, where $\text{disc}(K|F)$ denotes the discriminant. For this case, we have a specific notation:

Definition 39. If $K|F$ is abelian and $\mathfrak{p} \nmid \text{disc}(K|F)$, then the Frobenius automorphism $\text{Frob} = \left[\frac{K}{\mathfrak{P}} \right]$ depends only on the prime ideal \mathfrak{p} in F below \mathfrak{P} and is uniquely determined by (1.12). It is called the *Artin automorphism of \mathfrak{p} in $K|F$* and is denoted by

$$\text{Frob} = \left(\frac{K}{\mathfrak{p}} \right) = \left(\frac{K|F}{\mathfrak{p}} \right) \quad (\text{Artin symbol}).$$

We will now prove some theorems about this Artin symbol, which will be fundamental for subsequent investigations. Most of these theorems have analogs for the Frobenius symbol and then play a similar role in a general theory. We will restrict ourselves, however, to the abelian case, which is the only case we will need.

Since $(\frac{K}{\mathfrak{p}})$ generates the decomposition group, its order is equal to the order of G_Z and therefore equal to the inertia degree f of the prime ideal factor \mathfrak{P} in K of \mathfrak{p} . In particular, $(\frac{K}{\mathfrak{p}}) = 1$ means that $G_Z = 1$, i.e., that all \mathfrak{P} have degree 1, hence that \mathfrak{p} splits completely in K . We formulate this explicitly:

Theorem 40. *The order of $(\frac{K}{\mathfrak{p}})$ is equal to the inertia degree of $\mathfrak{P}|\mathfrak{p}$; in particular, we have $(\frac{K}{\mathfrak{p}}) = 1$ if and only if \mathfrak{p} splits completely in K .*

Now we will investigate how the Artin symbol for \mathfrak{p} behaves upon replacing K by a subextension L of $K|F$. Let $\mathfrak{p} \nmid \text{disc}(K|F)$. If L is a subextension of $K|F$, then $\mathfrak{p} \nmid \text{disc}(L|F)$, since $\text{disc}(L|F) \mid \text{disc}(K|F)$. Thus if $(\frac{K}{\mathfrak{p}})$ is defined, then so is $(\frac{L}{\mathfrak{p}})$. Let H be the invariant group of L , that is, the group of all automorphisms of $K|F$ that fix the elements of L . From

$$\alpha^{(K/\mathfrak{p})} \equiv \alpha^{N_{\mathfrak{p}}} \pmod{\mathfrak{p}}$$

for all \mathfrak{p} -integral $\alpha \in K$ it then follows that

$$\alpha^{H \cdot (K/\mathfrak{p})} \equiv \alpha^{N_{\mathfrak{p}}} \pmod{\mathfrak{p}}$$

for all those α that even lie in L . Since the factor group G/H is the Galois group of $L|F$ (or rather is isomorphic to it), we have found the Artin automorphism for L which is uniquely determined by this congruence: $(\frac{L}{\mathfrak{p}}) = H(\frac{K}{\mathfrak{p}})$ in the sense that all automorphisms of $H(\frac{K}{\mathfrak{p}})$ induce the Artin automorphism in L . Thus we have

Theorem 41. *If L is a subextension of the abelian extension $K|F$ with invariant group H . Then, for every $\mathfrak{p} \nmid \text{disc}(K|F)$,*

$$\left(\frac{L}{\mathfrak{p}}\right) = H \cdot \left(\frac{K}{\mathfrak{p}}\right).$$

Applying Theorem 40 this yields the following: the automorphisms of H induce the identity on L : the statement that $(\frac{K}{\mathfrak{p}}) \in H$ therefore means that the Artin symbol of \mathfrak{p} for $L|F$ is the identity, and according to Theorem 40 this means that \mathfrak{p} splits completely in L . Thus we have

Addition (to Theorem 41). *The prime ideal \mathfrak{p} splits completely in L if and only if $(\frac{K}{\mathfrak{p}})$ belongs to H .*

We now shall derive two formulas describing the behaviour of the Artin symbol under composition of the top fields and extension of the base field. First let K_1, K_2 be two independent (i.e., $K_1 \cap K_2 = F$) abelian extensions of F . Then we know that $K = K_1 K_2$ is abelian over F and that the Galois group of K is the direct product $G = G_1 \times G_2$ of the Galois groups G_1 and G_2 of K_1 and K_2 in the sense that $\sigma_1 \sigma_2$ with $\sigma_1 \in G_1$ and $\sigma_2 \in G_2$ denotes

the unique automorphism of K that acts as σ_1 on elements of K_1 and as σ_2 on elements of K_2 . Thus the automorphisms σ_1 act trivially on K_2 , and the σ_2 act trivially on K_1 . Now let \mathfrak{p} be a prime ideal of F with $\mathfrak{p} \nmid \text{disc}(K_1|F)$ and $\mathfrak{p} \nmid \text{disc}(K_2|F)$, so that $(\frac{K_1}{\mathfrak{p}})$ and $(\frac{K_2}{\mathfrak{p}})$ are defined. We want to show that a) $(\frac{K_1K_2}{\mathfrak{p}}) = (\frac{K}{\mathfrak{p}})$ is also defined and b) study how $(\frac{K}{\mathfrak{p}})$ is composed from $(\frac{K_1}{\mathfrak{p}})$ and $(\frac{K_2}{\mathfrak{p}})$.

For a) we have to show, using Dedekind's discriminant theorem, that \mathfrak{p} is unramified in $K = K_1K_2$ if it is unramified in K_1 and K_2 . We will prove a little bit more; this will not make the proof more difficult but somewhat more transparent. Thus let K_1 and K_2 be two arbitrary Galois extensions (not necessarily abelian). If \mathfrak{p} is unramified [splits completely] in K , then the multiplicativity of inertia degree and ramification index shows that \mathfrak{p} is unramified [splits completely] in K_1 and K_2 . Now assume conversely that \mathfrak{p} is unramified [splits completely] in K_1 and K_2 , and let \mathfrak{P} be a prime divisor of \mathfrak{p} in K . The inertia field (decomposition field) of \mathfrak{P} contains by the maximality property (Theorem 31) both K_1 and K_2 . Thus it contains the compositum K , hence is equal to K , and therefore \mathfrak{p} is unramified [splits completely] in K .

As a matter of fact we can extend this result without problems to arbitrary algebraic number fields of finite degree over F . To this end it only remains to show that \mathfrak{p} is unramified [splits completely] in an arbitrary field K if and only if it is unramified [splits completely] in the associated Galois closure K^* . Again the behaviour of \mathfrak{p} in K^* immediately implies the same behaviour of \mathfrak{p} in K . Conversely, if \mathfrak{p} is unramified [splits completely] in K , then the same is true for the conjugate fields $K^{(\nu)}$ of K over F . The inertia field (decomposition field) of a prime factor \mathfrak{P} of \mathfrak{p} in K^* thus has to contain all conjugate fields $K^{(\nu)}$, hence has to be equal to K^* . Thus \mathfrak{p} is unramified [splits completely] in K^* . We have proved the following result:

Theorem 42. *Let K_1, K_2 be two arbitrary finite algebraic extensions of F ; then a prime ideal \mathfrak{p} in F splits completely (is unramified) in the compositum $K = K_1K_2$ if and only if the same is true in K_1 and K_2 .*

b) We now put $(\frac{K}{\mathfrak{p}}) = \sigma_1\sigma_2$ with $\sigma_1 \in G_1$ and $\sigma_2 \in G_2$. This allows us to determine $(\frac{K_1}{\mathfrak{p}})$ and $(\frac{K_2}{\mathfrak{p}})$ because here we are in the situation of Theorem 41. Its application yields: $(\frac{K_1}{\mathfrak{p}}) = G_2 \cdot (\frac{K}{\mathfrak{p}})$, since G_2 is the invariant group of K_1 within K . This shows that $(\frac{K_1}{\mathfrak{p}})$ is the automorphism that is induced by $(\frac{K}{\mathfrak{p}})$ in K_1 , and by definition of the direct product this is just σ_1 ; thus $(\frac{K_1}{\mathfrak{p}}) = \sigma_1$. Similarly, we have $(\frac{K_2}{\mathfrak{p}}) = \sigma_2$ and $(\frac{K}{\mathfrak{p}}) = (\frac{K_1}{\mathfrak{p}})(\frac{K_2}{\mathfrak{p}})$. We have proved:

Theorem 43. *Let K_1, K_2 be independent abelian extensions of F , and let G_1, G_2 be their Galois groups; if G_1 fixes the elements of K_2 and G_2 those of K_1 , then for all $\mathfrak{p} \nmid \text{disc}(K_1|F)$, $\mathfrak{p} \nmid \text{disc}(K_2|F)$, and hence for all $\mathfrak{p} \nmid \text{disc}(K_1K_2|F)$, we have*

$$\left(\frac{K_1 K_2}{\mathfrak{p}}\right) = \left(\frac{K_1}{\mathfrak{p}}\right) \left(\frac{K_2}{\mathfrak{p}}\right).$$

We now want to study the behaviour of the Artin symbol under extension of the base field F . Let $\overline{F}|F$ be an extension of finite degree, and let $\overline{K} = K \cdot \overline{F}$. Let \mathfrak{p} be a prime ideal in F , $\overline{\mathfrak{p}}$ a prime factor of \mathfrak{p} in \overline{F} . In order to be able to say something about the Artin symbols we first have to show that if \mathfrak{p} is unramified in K , then so is $\overline{\mathfrak{p}}$ in \overline{K} . To this end we consider a more general situation: let K be an arbitrary Galois extension of F ; then \overline{K} is Galois over \overline{F} . Let \mathfrak{P} be a prime ideal in K and $\overline{\mathfrak{P}}$ a prime factor of \mathfrak{P} in \overline{K} , and let \mathfrak{p} , $\overline{\mathfrak{p}}$ be the corresponding prime ideals in F and \overline{F} .

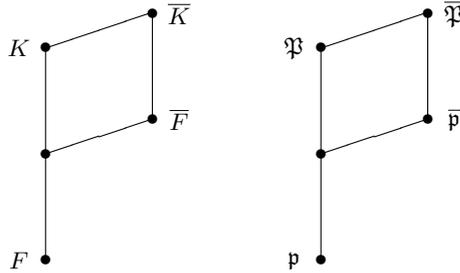


Fig. 1.7.

If \mathfrak{P} is unramified [splits completely] in $K|F$, then the inertia subgroup G_T [the decomposition group G_Z] of \mathfrak{P} is trivial. Now every element of the inertia subgroup \overline{G}_T [decomposition group \overline{G}_Z] of $\overline{\mathfrak{P}}$ over \overline{F} fixes the residue classes modulo \mathfrak{P} in K [the prime ideal \mathfrak{P}]; thus its restriction to K fixes the residue classes modulo the prime factor \mathfrak{P} in K [the prime ideal \mathfrak{P}]. If we use the natural isomorphism to identify the automorphisms of $\overline{K}|\overline{F}$ with the induced automorphisms of $K|F$, then it follows that

$$\overline{G}_T \subseteq G_T \quad [\overline{G}_Z \subseteq G_Z],$$

and since $G_T = 1$ [$G_Z = 1$] we get $\overline{G}_T = 1$ [$\overline{G}_Z = 1$]. Therefore $\overline{\mathfrak{P}}$ is unramified [splits completely] in $\overline{K}|\overline{F}$.

Assuming even more generally that K is an arbitrary extension of finite degree over F , then using the normal closure $K^*|F$ of $K|F$ and the compositum $\overline{K}^* = K^* \cdot \overline{F}$ together with the remark in the last paragraph before Theorem 42 we get exactly the same result. Thus we may formulate:

Theorem 44. *If $K|F$ and $\overline{F}|F$ are finite extensions, moreover $\overline{K} = K \cdot \overline{F}$ and \mathfrak{P} a prime ideal in K that is unramified [splits completely] in $K|F$, then every prime ideal $\overline{\mathfrak{P}}$ above \mathfrak{P} is unramified [splits completely] in $\overline{K}|\overline{F}$.*

Now assume that $K|F$ is abelian. If \mathfrak{p} is unramified in K , then by the theorem above $\overline{\mathfrak{p}}$ will be unramified in \overline{K} , that is, if $\left(\frac{K}{\mathfrak{p}}\right)$ is defined, then so

is $\left(\frac{\overline{K}}{\overline{\mathfrak{p}}}\right)$. The last symbol is defined by the congruence

$$\overline{\alpha}^{(\overline{K}/\overline{\mathfrak{p}})} \equiv \overline{\alpha}^{N\overline{\mathfrak{p}}} \pmod{\overline{\mathfrak{p}}} \quad \text{for all } \overline{\mathfrak{p}}\text{-integral } \overline{\alpha} \in \overline{K}.$$

In particular it follows for all integers $\alpha \in K$, if $\overline{\mathfrak{p}}$ has inertia degree r with respect to \mathfrak{p} , i.e., if $N\overline{\mathfrak{p}} = N(\mathfrak{p})^r$, that

$$\alpha^{(\overline{K}/\overline{\mathfrak{p}})} \equiv \alpha^{N\mathfrak{p}^r} \pmod{\mathfrak{p}}.$$

Applying the defining congruence for $\left(\frac{K}{\mathfrak{p}}\right)$ r times we find

$$\alpha^{(K/\mathfrak{p})^r} \equiv \alpha^{N(\mathfrak{p})^r} \pmod{\mathfrak{p}}.$$

Since the Artin symbol is uniquely determined by this congruence, we find, in the sense of the natural isomorphism, that

$$\left(\frac{\overline{K}}{\overline{\mathfrak{p}}}\right) = \left(\frac{K}{\mathfrak{p}}\right)^r.$$

We have proved:

Theorem 45 (Escalator Theorem for the Artin Symbol). *Let $K|F$ be an abelian extension, $\overline{F}|F$ an arbitrary finite extension, and put $\overline{K} = K\overline{F}$. Assume moreover that $\mathfrak{p} \nmid \text{disc}(K|F)$ and that $\overline{\mathfrak{p}}$ is a prime ideal in \overline{F} above \mathfrak{p} with inertia degree r relative to \mathfrak{p} .*

Then $\overline{\mathfrak{p}} \nmid \text{disc}(\overline{K}|\overline{F})$ and

$$\left(\frac{\overline{K}/\overline{F}}{\overline{\mathfrak{p}}}\right) = \left(\frac{K}{\mathfrak{p}}\right)^r.$$

We explicitly mention the case where \overline{F} is a subfield of K_j .

Addition to Theorem 45. *If L is a subfield of the abelian field K over F and if \mathfrak{q} is a prime ideal in L above \mathfrak{p} with $\mathfrak{p} \nmid \text{disc}(K|F)$ and with inertia degree r over \mathfrak{p} , then*

$$\left(\frac{K/L}{\mathfrak{q}}\right) = \left(\frac{K}{\mathfrak{p}}\right)^r.$$

With this result we for now leave the theory of Galois and abelian extensions.