Chapter 6

Dedekind Schemes

In this chapter we introduce the main protagonists of the following two chapters, namely Dedekind schemes. These will be schemes characterised by certain special properties that are common to smooth algebraic curves and spectra of rings of integers in number fields. Analogies between algebraic numbers and functions on algebraic curves have already been noticed in the 19th century; since then, several axiomatisations of the common features have been proposed of which the notion of a Dedekind scheme seems to be particularly satisfactory.

1. Integral Extensions

In this section we review the basic theory of integral extensions of rings. As this topic is well treated in many texts (e.g. in the books of Lang [1], [2]), we include proofs only for the easiest facts.

Recall that given an extension of rings $A \subset B$, an element $b \in B$ is said to be *integral* over A if it is a root of a *monic* polynomial $x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in A[x]$. There is the following well-known characterisation of integral elements:

Lemma 1.1 *Let $A \subset B$ an extension of rings. Then the following are equivalent for an element $x \in B$:*

1. *The element x is integral over A.*
2. *The subring $A[x]$ of B is finitely generated as an A-module.*
3. *There is a subring C of B containing x which is finitely generated as an A-module.*

Proof: For the implication 1) $\Rightarrow$ 2) note that if x satisfies a monic polynomial of degree n, then $1, x, \ldots, x^{n-1}$ is a basis of $A[x]$ over A. The implication 2) $\Rightarrow$ 3) being trivial, only 3) $\Rightarrow$ 1) remains. For this consider the A-module endomorphism of C given by multiplication by x. Its characteristic polynomial f is monic; by the Cayley-Hamilton theorem, $f(x) = 0$. □

Corollary 1.2 *Those elements of B which are integral over A form a subring in B.*

Proof: Indeed, given two elements $x, y \in B$ integral over A, the elements $x-y$ and xy are both contained in the subring $A[x, y]$ of B which is a finitely generated A-module by assumption. □

If all elements of B are integral over A, we say that the extension $A \subset B$ is *integral.*

Corollary 1.3 *Given a tower extensions $A \subset B \subset C$ with $A \subset B$ and $B \subset C$ integral, the extension $A \subset C$ is also integral.*

If A is a domain with fraction field K and L is an extension of K, the *integral closure* of A in L is the subring of L formed by elements integral over A. We say that A is *integrally closed* if its integral closure in the fraction field K is just A. By the corollary above, the integral closure of a domain A in some extension L of its fraction field is integrally closed.

Example 1.4 Any unique factorisation domain A is integrally closed. Indeed, if an element $a/b \in K$ (with a, b coprime) satisfies a monic polynomial equation of degree n, then by multiplying with b^n we see that a^n should be divisible by b which is only possible when b is a unit.

In particular, the ring $\mathbf{Z}$ is integrally closed.

Recall that a *number field* K is by definition a finite extension of $\mathbf{Q}$. We denote by $\mathcal{O}_K$ the integral closure of $\mathbf{Z}$ in K and call it the *ring of integers of K*. Of course, $\mathcal{O}_K$ is integrally closed.

We next collect some easy results that will be needed in subsequent sections.

Lemma 1.5 *Let $A \subset B$ be an integral extension of domains.*

1. *If I is a nonzero ideal of B, then $I \cap A$ is a nonzero ideal of A.*

2. *If A is a field, then B is a field as well.*

Proof: For the first statement note that if a nonzero $u \in I$ satisfies an equation $u^n + a_{n-1}u^{n-1} + \ldots + a_1u + a_0 = 0$ with $a_i \in k$, then $a_0 \in I \cap A$. Since B is a domain, we may assume $a_0 \neq 0$, whence the assertion. The second statement follows from this for if I is a nonzero ideal of B, we must have $I \cap A = A$ when A is a field, hence $1 \in I$ and $I = B$. □

Remark 1.6 In fact, the converse of the second statement is also true: if B is a field, then A must be a field as well, but we shall not need this.

Lemma 1.7 *A domain A is integrally closed if and only if for any prime idal P of A the localisation A_P is integrally closed.*

Proof: Denote by K the fraction field of A. One implication is easy: if an element $x \in K$ satisfies a monic equation over A_P, then by multiplying with a suitable common multiple s of the denominators of the coefficients one gets that sx is integral over A, hence $sx \in A$. For the converse, take an element $x = a/b \in K$ integral over A. If b is not a unit in A, there is some maximal ideal P containing it. But A_P is integrally closed and a/b is integral over it, so $a/b \in A_P$ which is absurd. Thus b is a unit and $a/b \in A$. □

Finally, a similar argument to that in the first part of the previous proof shows:

Lemma 1.8 *Let A be a domain with fraction field K ans let $S \subset A$ be a multiplicatively closed subset. Then for any field extension $L|K$, the integral closure of the localisation A_S in L is B_S, where B is the integral closure of A in L.*

The last topic to be treated in this section is the question whether the integral closure of an integral domain A in a finite extension of its fraction field is a finitely generated A-module. Unfortunately, this property does not hold for arbitrary domains, even under the assumption that A is noetherian. But there are two classical sufficient conditions which we now quote from the literature.

Proposition 1.9 *Let A be an integrally closed noetherian domain with fraction field K and let L be a finite separable extension of K. Then the integral closure B of A in any finite extension of L is a finitely generated A-module, and hence a Noetherian ring.*

For the proof, see Atiyah-Macdonald [1], Corollary 5.17 or Lang [2], Chapter I, Proposition 6.

The other sufficient condition is the following.

Proposition 1.10 *Let k be a field and A an integral domain which is a finitely generated k-algebra. If L is any finite extension of the fraction field K of A, then the integral closure of A in L is a finitely generated A-module.*

Note that the proposition is implied by the previous one when k is of characteristic 0. In the case of positive characteristic, there is a simple proof for polynomial rings in Shafarevich [1], Appendix, Section 8. The general case reduces to this case by applying Noether's Normalisation Lemma (Lang [1], Chapter VIII, Theorem 2.1).

2. Dedekind Schemes

We begin the discussion of Dedekind schemes by studying their local rings which enjoy very similar properties to rings of germs of meromorphic functions in a neighbourhood of some point of a Riemann surface. The first of the several equivalent definitions we are to give is perhaps the simplest one.

Definition 2.1 A ring A is a *discrete valuation ring* if A is a local principal ideal domain which is not a field.

Before stating the first equivalent characterisations, observe that if A is a local ring with maximal ideal P, then the A-module P/P^2 is in fact a vector space over the field $\kappa(P) = A/P$, simply because multiplication by P maps P into P^2.

Proposition 2.2 *For a local domain A with maximal ideal P the following conditions are equivalent:*

1. *A is a discrete valuation ring.*
2. *A is noetherian of Krull dimension 1 and P/P^2 is of dimension 1 over $\kappa(P)$.*
3. *A is noetherian and P is generated by a single nonzero element.*

For the proof we need the following well-known lemma which will be extremely useful in other situations as well:

Lemma 2.3 (Nakayama's Lemma) *Let A be a local ring with maximal ideal P and M a finitely generated A-module. If $PM = M$, then $M = 0$.*

Proof: Assume $M \neq 0$ and let $m_0, \ldots, m_n$ be a minimal system of generators of M over A. By assumption m_0 is contained in PM and hence we have a relation $m_0 = p_0 m_0 + \ldots, p_n m_n$ with all the p_i elements of P. But here $1 - p_0$ is a unit in A (as otherwise it would generate an ideal contained in P) and hence by multiplying the equation by $(1-p_0)^{-1}$ we may write m_0 as a linear combination of the other terms, which is in contradiction with the minimality of the system. □

Here is an immediate corollary of the lemma.

Corollary 2.4 *Let A be a Noetherian local ring with maximal ideal P. Then*

$$\bigcap_i P^i = (0).$$

Moreover, if $P^i \neq (0)$, then $P^i \neq P^{i+1}$.

Proof: Denote by Q the intersection of the P^i. Since A is Noetherian, Q is finitely generated. Moreover, $PQ = Q$ and the lemma applies. The second statement is proved in a similar way. □

Another corollary of the lemma is the following strengthened form.

Corollary 2.5 *Let A, P, M be as in the lemma and assume given elements $t_1, \ldots, t_m \in M$ whose images in the A/P-vector space M/PM form a generating system. Then they generate M over A.*

Proof: Let T be the A-submodule generated by the t_i; we have $M = T + PM$ by assumption. Hence $M/T = P(M/T)$ and the lemma gives $M/T = 0$. □

Proof of Proposition 2.2: Assume A is a discrete valuation ring and P is generated by t. Then by Corollary 2.4 any nonzero prime ideal $Q \subset P$ must contain a power of t. But being a prime ideal, it must then contain t itself, so that $Q = P$ and A is of Krull dimension one. Also, the image of t generates the vector space P/P^2, whence the second condition. The third condition follows from the second by applying Corollary 2.5 with $M = P$. Finally, to show that the third condition implies the first, assume the maximal ideal P of A is generated by some element t. We first show that any element $a \in A$ can be written uniquely as a product $a = ut^n$, with u a unit in A. Indeed, by Corollary 2.4 there is a unique $n \geq 0$ for which $a \in P^n \setminus P^{n+1}$ and thus a can be written in the required form. If $a = ut^n = vt^n$, then $u = v$ since A is a domain. Now take an ideal I of A. As A is Noetherian, I can be generated by a finite sequence of elements $a_1, \ldots, a_k$. Write $a_i = u_i t^{n_i}$ according to the above representation and let j be an index for which $n_i \geq n_j$ for all i. Each a_i is a multiple of t^{n_j} and hence $I = (t^{n_j})$ is principal. □

In the course of the above proof we have also shown:

Corollary 2.6 *Any element $x \neq 0$ of the fraction field of a discrete valuation ring A can be written uniquely in the form $x = ut^n$ with u a unit in A, t a generator of the maximal ideal and n a (possibly negative) integer.*

The second condition of the lemma may seem a bit technical, but it is very useful for it is a special case of a more general notion coming from algebraic geometry.

Definition 2.7 A noetherian local ring A with maximal ideal P is *regular* if its Krull dimension equals the (finite) dimension of P/P^2 over $\kappa(P)$.

Thus discrete valuation rings are regular local rings of dimension 1.

We now explain the origin of the name "discrete valuation ring".

Definition 2.8 For any field K, a *discrete valuation* is a surjection $v : K \to \mathbf{Z} \cup \{\infty\}$ with the properties

$$v(xy) = v(x) + v(y),$$

$$v(x + y) \geq \min\{v(x), v(y)\},$$

$$v(x) = \infty \text{ if and only if } x = 0.$$

The elements $x \in K$ with $v(x) \geq 0$ form a subring $A \subset K$ called the *valuation ring* of v.

Proposition 2.9 *A domain A is a discrete valuation ring if and only if it is the valuation ring of some discrete valuation $v : K \to \mathbf{Z} \cup \{\infty\}$, where K is the fraction field of A.*

Proof: Assume first A is a discrete valuation ring. Define a function $v : K \to \mathbf{Z} \cup \{\infty\}$ by mapping 0 to ∞ and any $x \neq 0$ to the integer n given by the previous corollary. It is immediate to check that v is a discrete valuation with valuation ring A. Conversely, given a discrete valuation v on K, the maximal ideal of its valuation ring is generated by any t with $v(t) = 1$ and we may apply the previous proposition. □

We can now discuss the example mentioned at the beginning of this section.

Example 2.10 Let $\mathcal{M}$ be the sheaf of meromorphic functions on some Riemann surface X and x a point of X. Define $v(f) = m$ if f is holomorphic at x and has a zero of order m and define $v(f) = -v(1/f)$ otherwise. Then v is a discrete valuation on $K = \mathcal{M}(X)$ whose discrete valuation ring is the stalk of $\mathcal{M}$ at x.

The last characterisation of discrete valuation rings we shall need is the following.

Proposition 2.11 *A domain A is a discrete valuation ring if and only if A is noetherian, integrally closed and has a unique nonzero prime ideal.*

For the proof, which we have taken from Serre [1], we need a technical lemma.

Lemma 2.12 *Let A be a domain having a unique nonzero prime ideal P. Then $P^{-1} \neq A$.*

Here P^{-1} denotes the set of elements x of the fraction field K of A with $xA \subset P$.

Proof: Observe first that for any $f \in P$ the localisation A_f is a field and hence equals K itself. Indeed, for a maximal ideal M of A_f the prime ideal $M \cap A$ doesn't contain f, hence it can be only (0). But for any nonzero element $y/f^n \in M$ we would have $0 \neq y \in M \cap A$, whence $M = 0$, as desired. Take now another $x \in P$; by the above we may write $x^{-1} = a/f^m$ with some m, so $f^m = ax$, and thus $f^m \in (x)$. Letting f vary in a finite set of generators of P we conclude that a sufficiently high power of P is contained in (x). Let P^N be the least such power; we may thus find $y \in P^{N-1}$ with $y \notin (x)$. But $yP \subset (x)$, so $yx^{-1} \in P^{-1}$. However, $yx^{-1} \notin A$ as $y \notin (x)$. □

Proof of Proposition 2.11: The necessity of the conditions is immediate (the second condition follows from Example 1.4 and the last from the fact that any nonzero ideal of A is of the form (t^n) with t a generator of the maximal ideal; such an ideal can be prime only for $n = 1$).

For sufficiency denote by P the maximal ideal of A; we have to show that it is principal. Evidently $A \subset P^{-1}$, so $P \subset P^{-1}P$, the latter being the ideal of A generated by elements of the form xy with $x \in P^{-1}$ and $y \in P$. Since P is maximal, there are two cases: either $P^{-1}P = A$ or $P^{-1}P = P$. We now show that if the first case holds, then P is principal. Indeed, in this case there is a relation of the form $x_1y_1 + \ldots + x_ny_n = 1$ with $x_i \in P^{-1}$ and $y_i \in P$. Here there is at least one i for which $x_iy_i \notin P$, so there is some unit

u with $ux_iy_i = 1$. We contend that $P = (y_i)$. Indeed, if $z \in P$, we have $z = uzx_iy_i$, but $uzx_i \in A$ since $x_i \in P^{-1}$.

To finish the proof we show that the case $P^{-1}P = P$ cannot occur. We do this by showing that this assumption implies $P^{-1} = A$, in contradiction with lemma 2.12. So take $x \in P^{-1}$. By assumption $xP \subset P$; iterating this we get $x^nP \subset P$ for all n, so $x^n \in P^{-1}$ for all n. In particular, for any $f \in P$ all powers of x are contained in the A-submodule of K generated by f^{-1}, which is a finitely generated A-module. But A is noetherian and a submodule of a finitely generated module over a noetherian ring is always finitely generated, hence by Lemma 1.1 x is integral over A. As A is integrally closed, this implies $x \in A$, as desired. □

Remark 2.13 The affine scheme $\operatorname{Spec} A$ is particularly simple for a discrete valuation ring. It consists only two points, a closed point x (corresponding to the maximal ideal) and a non-closed generic point η (corresponding to the ideal (0)). The stalk of the structure sheaf at η is the fraction field K of A and the stalk at x is A itself.

Now we can pass from local rings to schemes and give our main definition.

Definition 2.14 A *normal scheme* is a scheme whose local rings are integrally closed domains. A *Dedekind scheme* is an integral noetherian normal scheme of dimension 1. A *Dedekind ring* is a domain A such that $\operatorname{Spec} A$ is a Dedekind scheme.

Remarks 2.15 Here some remarks are in order.

1. There is another restriction that is convenient to impose on the schemes we shall be looking at, namely that the local rings of X should be *distinct* when viewed as subrings of the function field K; in this case one says X is *separated (over* $\mathbf{Z}$). This condition plainly holds in the affine case where the local rings are all localisations at different prime ideals; it also holds for closed subschemes of projective space. However, there is a pathological example, the "affine line with the origin doubled" which satisfies the definition of a Dedekind scheme given above but which is not separated. This is constructed by taking two copies of the affine line $\mathbf{A}^1_k$ over some field k and patching them over the open subset $D(x)$ using the isomorphism given by the identity map. In this way we get two closed points coming from the two origins whose local rings are the same.

   Henceforth we shall tacitly assume that *all integral schemes under consideration are separated.*

2. Call a noetherian scheme *regular* if all of its local rings are regular. Then by Proposition 2.2 Dedekind schemes are precisely regular integral schemes of dimension 1.

Now let us draw some immediate consequences from the definition of Dedekind schemes.

Proposition 2.16 *Let X be a Dedekind scheme with function field K.*

1. *The closed subsets of X are just X and finite sets of closed points.*
2. *The local rings of X at closed points are discrete valuation rings with fraction field K.*
3. *Any affine open subset of X is of the form* $\operatorname{Spec} A$*, with A an integrally closed domain.*

Proof: Since X is noetherian, it is compact, so for the first statement we may assume $X = \operatorname{Spec} A$ with a Noetherian ring A. In $\operatorname{Spec} A$ any closed subset is a finite union of irreducible closed subsets. (To see this, decompose any reducible closed subset Z as a union of nonempty closed subsets $Z_1 \cup Z_2$; if these are not irreducible, decompose them again - the process must terminate in finitely many steps as otherwise we would get an infinite strictly increasing chain of ideals of A which is impossible in a noetherian ring.) But any irreducible closed subset of X is a closed point by Chapter 5, Lemma 6.13 and the fact that all prime ideals of A are maximal. This proves the first statement; the second follows from Proposition 2.11 in view of the easy fact that any localisation of a noetherian ring A is noetherian (as the ideals of the localisation are all generated by ideals of A according to Chapter 4, Lemma 2.4). The third is a consequence of Lemma 1.7. □

Examples 2.17 We now give the two main examples of Dedekind schemes.

1. Let $\mathcal{O}_K$ be the ring of integers of some number field K. Then $\operatorname{Spec} \mathcal{O}_K$ is a Dedekind scheme.

   Indeed, A is a domain, so $\operatorname{Spec} A$ is integral. That it is noetherian follows from Proposition 1.9. To prove that it is of dimension 1, we show that any nonzero prime ideal P of $\mathcal{O}_K$ is maximal. Indeed, by the first part of Lemma 1.5, the intersection $P \cap \mathbf{Z}$ is nonzero, hence generated by some prime number p. Now the induced extension $\mathbf{Z}/p\mathbf{Z} \subset \mathcal{O}_K/P$ is still integral, so we may apply the second statement of the same lemma to conclude that $\mathcal{O}_K/P$ is a field. Finally the normality of $\operatorname{Spec} A$ follows from Lemma 1.7.

2. The second basic example of a Dedekind scheme is given a by one-dimensional normal integral closed subscheme of affine (resp. projective) n-space over some field k. These we shall call *smooth affine (resp. projective) curves* over k. For the moment, this definition is tautologous but one can still give some concrete examples. For instance, the affine line $\mathbf{A}_k^1$ is a smooth affine curve (being the spectrum of the one-dimensional unique factorisation domain $k[t]$) and the projective line $\mathbf{P}_k^1$ is a smooth projective curve over k for it is integral and can be covered by two copies of $\mathbf{A}_k^1$.

However, for a general closed subscheme of affine or projective space this ring-theoretic definition in the second example is rather hard to check. What is much more preferable is the smoothness condition encountered in our discussion of Riemann surfaces; for a plane curve this said that the partial derivatives of its defining equation should not simultaneously vanish at some point. In the next section we introduce an algebraic formalisation of the notion of differentials and prove a broad generalisation of this criterion.

3. Modules and Sheaves of Differentials

In differential geometry, the tangent space at a point P on some variety is defined to consist of so-called *linear derivarions*, i.e. linear maps that associate a scalar to each function germ at P and satisfy the Leibniz rule. We begin by an algebraic generalisation of this notion.

Definition 3.1 Let B be a ring and M a B-module. A *derivation* of B into M is a map $d:\ B \to M$ subject to the two conditions:

1. (Additivity) $d(x+y) = dx + dy$;

2. (Leibniz rule) $d(xy) = xdy + ydx$.

Here we have written dx for $d(x)$ to emphasise the analogy with the classical derivation rules. If moreover B is an A-algebra for some ring A (for example $A = \mathbf{Z}$), an A-linear derivation is called an *A-derivation.* The set of A-derivations of B to M is equipped with a natural B-module structure via the rules $(d_1 + d_2)x = d_1x + d_2x$ and $bdx = dbx$. This B-module is denoted by $Der_A(B, M)$.

Note that applying the Leibniz rule to the equality $1 \cdot 1 = 1$ gives $d(1) = 0$ for all derivations; hence all A-derivations are trivial on the image of A in B.

In the example one encounters in (say) real differential geometry we have $A = M = \mathbf{R}$, and B is the ring of germs of differentiable functions at some point; $\mathbf{R}$ is a B-module via evaluation of functions. Now comes a purely algebraic example.

Example 3.2 Assume given an A-algebra B which decomposes *as an A-module* into a direct sum $B \cong A \oplus I$, where I is an ideal of B with $I^2 = 0$. Then the natural projection $d : B \to I$ is an A-derivation of B into I. Indeed, A-linearity is immediate; for the Leibniz rule we take elements $x_1, x_2 \in B$ and write $x_i = a_i + dx_i$ with $a_i \in k$ for $i = 1, 2$. Now we have

$$d(x_1x_2) = d[(a_1 + dx_1)(a_2 + dx_2)] = d(a_1a_2 + a_2dx_1 + a_1dx_2) = x_2dx_1 + x_1dx_2$$

where we used several times the facts that $I^2 = 0$ and $d(A) = 0$.

In fact, given any ring A and A-module I, we can define an A-algebra B as above by defining a product structure on the A-module $A \oplus I$ by the rule $(a_1, i_1)(a_2, i_2) = (a_1a_2, a_1i_2 + a_2i_1)$. So the above method yields plenty of examples of derivations.

Now notice that for fixed A and B the rule $M \to Der_A(B, M)$ defines a functor on the category of B-modules; indeed, given a homomorphism $\phi : M_1 \to M_2$ of B-modules, we get a natural homomorphism $Der_A(B, M_1) \to Der_A(B, M_2)$ by composing derivations with ϕ.

Proposition 3.3 *The functor $M \to Der_A(B, M)$ is representable by a B-module $\Omega_{B/A}$.*

Proof: The construction is done in a similar way to that of the tensor product of two modules. Define $\Omega_{B/A}$ to be the quotient of the free B-module generated by symbols dx for each $x \in B$ modulo the relations given by the additivity and Leibniz rules as in Definition 3.1 as well as the relations $d(\lambda(a)) = 0$ for all $a \in A$, where $\lambda : A \to B$ is the map defining the A-module structure on B. The map $x \to dx$ is an A-derivation of B into $\Omega_{B/A}$. Moreover, given any B-module M and A-derivation $\delta \in Der_A(B, M)$, the map $dx \to \delta(x)$ induces a B-module homomorphism $\Omega_{B/A} \to M$ whose composition with d is just δ. This implies that $\Omega_{B/A}$ represents the functor $M \to Der_A(B, M)$; in particular, d is the universal derivation corresponding to the identity map of $\Omega_{B/A}$. □

We call $\Omega_{B/A}$ the module of *relative differentials* of B with respect to A. We shall often refer to the elements of $\Omega_{B/A}$ as *differential forms.*

Next we describe how to compute relative differentials of a finitely presented A-algebra.

Proposition 3.4 *Let B be the quotient of the polynomial ring $A[x_1, \ldots, x_n]$ by an ideal generated by finitely many polynomials $f_1, \ldots, f_m$. Then $\Omega_{B/A}$ is the quotient of the free B-module on generators $dx_1, \ldots, dx_n$ modulo the B-submodule generated by the elements $\sum_j (\partial_j f_i) dx_j$ $(i = 1, \ldots, m)$, where $\partial_j f_i$ denotes the j-th (formal) partial derivative of f_i.*

Proof: First consider the case $B = A[x_1, \ldots, x_n]$. As B is the free A-algebra generated by the x_i, one sees that for any B-module M there is a bijection between $Der_A(B, M)$ and maps of the set $\{x_1, \ldots, x_n\}$ into B. This implies that $\Omega_{B/A}$ is the free A-module generated by the dx_i.

The general case follows from this in view of the easy observation that given any M, composition by the projection $A[x_1, \ldots, x_n] \to B$ induces an isomorphism of $Der_A(B, M)$ onto the submodule of $Der_A(A[x_1, \ldots, x_n], M)$ consisting of derivations mapping the f_i to 0. □

Next some basic properties of modules of differentials.

Lemma 3.5 *Let A be a ring and B an A-algebra.*

1. *(Direct sums) For any A-algebra B'*

$$\Omega_{(B \oplus B')/A} \cong \Omega_{B/A} \oplus \Omega_{B'/A}.$$

2. *(Exact sequence) Given a map of A-algebras $\phi : B \to C$, there is an exact sequence of C-modules*

$$\Omega_{B/A} \otimes_B C \to \Omega_{C/A} \to \Omega_{C/B} \to 0.$$

   In particular, if ϕ is surjective, we have a surjection $\Omega_{B/A} \otimes_B C \to \Omega_{C/A}$.

3. *(Base change) Given a ring homomorphism $A \to A'$, denote by B' the A'-algebra $B \otimes_A A'$. There is a natural isomorphism*

$$\Omega_{B/A} \otimes_B B' \cong \Omega_{B'/A'}.$$

4. *(Localisation) For any multiplicatively closed subset $S \subset B$ there is a natural isomorphism*

$$\Omega_{B_S/A} \cong \Omega_{B/A} \otimes_B B_S.$$

Proof: The first property is easy and left to the readers. For the second, note that for any C-module M we have a natural exact sequence

$$0 \to Der_B(C, M) \to Der_A(C, M) \to Der_A(B, M)$$

of C-modules isomorphic to

$$0 \to \mathrm{Hom}_C(\Omega_{C/B}, M) \to \mathrm{Hom}_C(\Omega_{C/A}, M) \to \mathrm{Hom}_B(\Omega_{B/A}, M).$$

The claim follows from this in view of the formal Lemma 3.8 of Chapter 0 and the isomorphism $\mathrm{Hom}_B(\Omega_{B/A}, M) \cong \mathrm{Hom}_C(\Omega_{B/A} \otimes_B C, M)$. This isomorphism is obtained by mapping a homomorphism $\Omega_{B/A} \to M$ to the composite $\Omega_{B/A} \otimes_B C \to M \otimes_B C \to M$ where the second map is multiplication; an inverse is given by composition with the natural map $\Omega_{B/A} \to \Omega_{B/A} \otimes_B C$. If the map $B \to C$ is onto, then any B-derivation is a C-derivation as well, so $\Omega_{B/C} = 0$ and the first map in the exact sequence is onto.

For base change, note first that the universal derivation $d : B \to \Omega_{B/A}$ is an A-module homomorphism and so tensoring it by A' we get a map

$$d' : B' \to \Omega_{B/A} \otimes_A A' \cong \Omega_{B/A} \otimes_B B \otimes_A A' \cong \Omega_{B/A} \otimes_B B'$$

which is easily seen to be an A'-derivation. Now any A'-derivation $\delta' : B' \to M'$ induces an A-derivation $\delta : B \to M'$ by composition with the natural map $B \to B'$. But δ factors as $\delta = \phi \circ d$, with a B-module homomorphism $\phi : \Omega_{B/A} \to M'$, whence a map $\phi' : \Omega_{B/A} \otimes_B B' \to M'$ constructed as above. Now one checks that $\delta' = \phi' \circ d'$ which means that $\Omega_{B/A} \otimes_B B'$ represents the functor $M' \mapsto Der_{A'}(B', M')$.

For the localisation property, given an A-derivation $\delta : B \to M$, we may extend it uniquely to an A-derivation $\delta_S : B_S \to M \otimes_B B_S$ by setting $\delta_S(b/s) = (\delta(b)s - b\delta(s)) \otimes (1/s^2)$. (We leave it to the reader to check that for $b'/s' = b/s$ we get the same result – this is much simpler in the case when there are no zero-divisors in S which is the only case we shall need.) This applies in particular to the universal derivation $d : B \to \Omega_{B/A}$, and one argues as in the previous case to show that any A-derivation $B_S \to M_S$ factors uniquely through d_S. □

As a first application of the theory of differentials we prove a characterisation of finite étale algebras over a field, to be used in forthcoming chapters.

Proposition 3.6 *Let k be a field and A a finite dimensional k-algebra. Then A is étale if and only if $\Omega_{A/k} = 0$.*

Proof: For necessity we may assume by compatibility of $\Omega_{A/k}$ with direct sums that A is a finite separable field extension L of k. Then by the theorem of the primitive element $A \cong k[x]/(f)$ with some polynomial $f \in k[x]$ and so by Proposition 3.4 the L-module $\Omega_{L/k}$ can be presented with a single generator dx and relation $f'dx = 0$. But since the extension is separable, the polynomials f and f' are relatively prime and hence the image of f' in $L \cong k[x]/(f)$ is not 0. Whence $dx = 0$ in $\Omega_{L/k}$ and so $\Omega_{L/k} = 0$.

For sufficiency, it is enough to show by virtue of Chapter 1, Proposition 1.2 that $A \otimes_k \bar{k}$ is étale over $\bar{k}$ with $\bar{k}$ an algebraic closure of k. So using the base change property of differentials we may assume k is algebraicaly closed. Moreover, using the direct sum property as above we may even assume that A is indecomposable. Denoting by I its ideal of nilpotent elements, Chapter 5, Proposition 2.16 gives that A/I is a field. Since k is algebraically closed, we cannot but have $A/I \cong k$ and so we have a decomposition $A \cong k \oplus I$ of A as a k-module. Now to finish the proof we show that assuming $I \neq 0$ implies $\Omega_{A/k} \neq 0$. For this it is enough to show by the surjectivity property in Lemma 3.5 (2) that $\Omega_{(A/I^2)/k} \neq 0$, so we may as well assume $I^2 = 0$. But then we are (up to change of notation) in the situation of Example 3.2 which shows that for $I \neq 0$ the projection $d : A \to I$ is a nontrivial k-derivation, which implies $\Omega_{A/k} \neq 0$. □

As a second application of differentials we give a criterion for a one-dimensional closed subscheme of affine or projective space to be a smooth curve. For this it is enough to check that all local rings at closed points are discrete valuation rings. Since the proof works more generally for regular local rings, we state the result in this context.

Proposition 3.7 *Let k be a perfect field and let A be a localisation of a finitely generated n-dimensional k-algebra at some closed point P. Then A is a regular local ring if and only if $\Omega_{A/k}$ is a free A-module of rank n. In particular, if $n = 1$, A is a discrete valuation ring if and only if $\Omega_{A/k}$ is free of rank 1.*

Remark 3.8 Explicitly, if A is a localisation of the k-algebra

$$B = k[x_1, \dots, x_d]/(f_1, \dots, f_m),$$

then Proposition 3.4 and the localisation property of differentials imply that the proposition amounts to saying that among the relations $\sum_j (\partial_j f_i) dx_j = 0$ there should be exactly $d - n$ linearly independent ones, which in turn is equivalent by linear algebra to the fact that the $k \times m$ "Jacobian" matrix $J = [\partial_j f_i]$ should have rank $d - n$. In fact, for $k = \mathbf{C}$ reducing the entries of

J modulo the maximal ideal of A gives just the classical Jacobian matrix of the closed subscheme of $\mathbf{C}^d$ defined by the equations $f_i = 0$ at the point P corresponding to A and the condition says that some open neighbourhood of P should be a complex manifold of dimension n.

For the proof of the proposition we need two lemmas from algebra. The first of these is a form of Hilbert's Nullstellensatz (which implies the one used in the previous chapter).

Lemma 3.9 *Let k be a field and let P be a maximal ideal in a finitely generated k-algebra A. Then the field A/P is a finite extension of k.*

For a proof, see Lang [1], Chapter IX, Corollary 1.2. See also Atiyah-Macdonald [1] for four different proofs.

The other lemma is from field theory.

Lemma 3.10 *Let k be a perfect field and let $K|k$ be a finitely generated field extension of transcendence degree n. Then there exist algebraically independent elements $x_1, \ldots, x_n \in K$ such that the finite extension $K|k(x_1, \ldots, x_n)$ is separable.*

For a proof, see Lang [1], Chapter VIII, Corollary 4.4.

Corollary 3.11 *In the situation of the lemma, the K-vector space $\Omega_{K/k}$ is of dimension n, a basis being given by the dx_i.*

Proof: We may write the field K as the fraction field of the quotient A of the polynomial ring $k[x_1, \ldots, x_n, x]$ by a single polynomial relation f. Here f is the minimal polynomial of a generator of the extension $K|k(x_1, \ldots, x_n)$ multiplied with a common denominator of its coefficients. Now according to Proposition 3.4 the A-module $\Omega_{A/k}$ has a presentation with generators $dx_1, \ldots, dx_n, dx$ and a relation in which dx has a nontrivial coefficient because $f' \neq 0$ by the lemma. The corollary now follows using Lemma 3.5 (4). □

Proof of Proposition 3.7: We give the proof under the additional assumption that there exists a subfield $k \subset k' \subset A$ that maps isomorphically onto the residue field $\kappa(P) = A/P$ by the projection $A \to A/P$. (Lemma 3.9 implies that this condition is trivially satisfied if k is algebraically closed.) In the remark below we shall explain how one can reduce the general case to this one.

Notice that since k is perfect and $k'|k$ is a finite extension by Lemma 3.9, we have $\Omega_{k'|k} = 0$ by Proposition 3.6 (or the previous corollary). Hence by applying Lemma 3.5 (2) (with our k in place of A, k' in place of B and A in place of C) we get $\Omega_{A/k} \cong \Omega_{A/k'}$, so we may as well assume $k = k' \cong \kappa(P)$.

In this case the k-module P/P^2 is canonically isomorphic to $\Omega_{A/k}/P\Omega_{A/k}$. Indeed, the latter k-vector space is immediately seen to represent the functor $M \to Der_k(A, M)$ for any k-vector space M viewed as an A-module via the quotient map $A \to A/P \cong k$. On the other hand, the above functor is also represented by P/P^2. To see this, note first that the Leibniz rule implies that any k-derivation $\delta : A \to M$ is trivial on P^2, hence we may as well assume $P^2 = 0$. But then we are in the situation of Example 3.2 and we may observe that δ factors uniquely as $\delta = \phi \circ d$, with d as in the quoted example and $\phi \in \mathrm{Hom}_k(P, N)$.

Now if $\Omega_{A/k}$ is free of rank n, then $\Omega_{A/k}/P\Omega_{A/k} \cong P/P^2$ has dimension n. For the converse, observe first that the previous isomorphism and the corollary to Nakayama's lemma (Corollary 2.5) gives that $\Omega_{A/k}$ can be generated as an A-module by n elements $dt_1, \dots, dt_n$. Were there a nontrivial relation $\sum f_i dt_i = 0$ in $\Omega_{A/k}$, by the localisation property of differentials this relation would survive in $\Omega_{K/k}$, contradicting Corollary 3.11. This implies that $\Omega_{A/k}$ is free. □

Remark 3.12 To reduce the general case of the proposition to the one discussed above it is convenient to use the completion $\hat{A}$ of A. This is the inverse limit of of the natural inverse system formed by the quotients A/P^n of A. There is a natural map $A \to \hat{A}$ which is injective for A noetherian by Corollary 2.4. The image of P gives a maximal ideal $\hat{P}$ of $\hat{A}$ with $\hat{P}^i/\hat{P}^{i+1} \cong P^i/P^{i+1}$ for all $i > 0$. If A is of dimension 1, the case $i = 1$ of this isomorphism together with Corollary 2.5 implies that A is a discrete valuation ring if and only if $\hat{A}$ is. In general, we get that $\hat{A}$ is regular if and only if A is regular, for one can prove (see Atiyah-Macdonald [1], Corollary 11.19) that the Krull dimension of A is the same as that of $\hat{A}$. Also, the base change property of differentials implies that $\Omega_{\hat{A}/k}$ is free of rank n if and only if $\Omega_{A/k}$ is.

Therefore it remains to see that $\hat{A}$ satisfies the condition at the beginning of the above proof. For this, let $f \in k[x]$ be the minimal polynomial of a (separable) generator α of the extension $\kappa(P)|k$; it is enough to lift α to a root of f in $\hat{A}$. This can be done by means of Hensel's lemma (see Chapter 7, Section 4).

In the remaining of this section we discuss quasi-coherent sheaves associated to modules of differentials. Namely, we shall define *sheaves of relative differentials* $\Omega_{Y/X}$ for certain classes of morphisms of schemes $Y \to X$. In fact, one may define these for any morphism $Y \to X$ but since we did not develop the necessary background we refer the interested readers to the excellent treatment in Mumford's notes [1] or to Section II.8 of Hartshorne [1]. What we propose instead is a more down-to-earth discussion of the special cases we shall need.

Construction 3.13 First, if $Y = \operatorname{Spec} B$ and $X = \operatorname{Spec} A$ are both affine, we define $\Omega_{Y/X}$ as the quasi-coherent sheaf $\tilde{\Omega}_{B/A}$. Notice that according to the localisation property of differentials, over a basic open set $D(g) = \operatorname{Spec} B_g$ of X the sheaf $\Omega_{Y/X}$ is given by the B_g-module $\Omega_{B_g/A}$.

Construction 3.14 Next assume we have a morphism $X \to \operatorname{Spec} k$ with an arbitrary scheme X; we shall use the abusive notation $\Omega_{X/k}$ for the corresponding sheaf of differentials which we now construct. For any affine open covering of X by subsets $U_i = \operatorname{Spec} A_i$ the rings A_i are all k-algebras and the sheaf $\Omega_{U_i/k} = \tilde{\Omega}_{A_i/k}$ is defined on U_i. Moreover, any basic open subset contained in $U_i \cap U_j$ is canonically isomorphic to both $(A_i)_{f_i}$ and $(A_j)_{f_j}$, whence an isomorphism $\Omega_{(A_i)_{f_i}/k} \cong \Omega_{(A_j)_{f_j}}/k$. These isomorphisms are compatible for inclusions of basic open sets, so the third statement of Chapter 5, Lemma 2.7 applies to give an isomorphism $(\Omega_{U_i/k})|_{U_i \cap U_j} \cong (\Omega_{U_j/k})|_{U_i \cap U_j}$. These latter isomorphisms in turn are compatible over triple intersections $U_i \cap U_j \cap U_k$ so we may patch the $\Omega_{U_i/k}$ together by the method of Chapter 5, Construction 5.3 (which adapts to the construction of quasi-coherent sheaves) to get $\Omega_{X/k}$. Finally one checks that if we use a different open covering we get an $\mathcal{O}_X$-module isomorphic to $\Omega_{X/k}$.

Remark 3.15 Let X be an affine or a projective variety of dimension n. Then Proposition 3.7 may be rephrased by saying that X is a regular scheme if and only if the stalk of the sheaf $\Omega_{X/k}$ at each point is free of rank n (for the generic point this follows by localisation). From the next section on, we shall call such sheaves *locally free* (see Lemma 4.3 below). Also, those X for which $\Omega_{X/k}$ is locally free are usually called *smooth* (over k).

In particular, an affine or projective variety of dimension 1 is a Dedekind scheme if and only if it is a smooth curve.

Construction 3.16 Finally, the other case where we shall use relative differentials is that of an *affine* morphism $\phi : Y \to X$. In this case X is covered by affine open subsets $U_i = \operatorname{Spec} A_i$ whose inverse images $V_i = \operatorname{Spec} B_i$ form an open covering of Y and the B_i are A_i-modules via the maps $\lambda_i : A_i \to B_i$ arising from ϕ. Take $f_i \in A_i$ and put $g_i = \lambda_i(f_i)$. Then the inverse image of the basic open set $D(f_i) = \operatorname{Spec} (A_i)_{f_i}$ is none but $D(g_i)$ which in turn is isomorphic to $\operatorname{Spec} (B_i \otimes_{A_i} (A_i)_{f_i})$; indeed, one checks easily that $(B_i \otimes_{A_i} (A_i)_{f_i})$

represents the functor defining the localisation $(B_i)_{g_i}$. Hence by the base change property of differentials we have canonical isomorphisms

$$\Omega_{V_i/U_i}(D(g_i)) = \Omega_{B_i/A_i} \otimes_{B_i} (B_i)_{g_i} \cong \Omega_{(B_i)_{g_i}/(A_i)_{f_i}} = \Omega_{D(g_i)/D(f_i)},$$

so we may patch the sheaves Ω_{V_i/U_i} together over inverse images of basic affine open subsets contained in $U_i \cap U_j$ by the same method as in the previous case.

4. Invertible Sheaves on Dedekind Schemes

In this section we shall study some special coherent sheaves of fundamental importance for both the arithmetic and the geometry of Dedekind schemes. Here is the basic definition.

Definition 4.1 A *locally free sheaf* on a scheme X is an $\mathcal{O}_X$-module $\mathcal{F}$ for which there exists an open covering $\mathcal{U} = \{U_i : i \in I\}$ of X such that the restriction of $\mathcal{F}$ to each U_i is isomorphic to $\mathcal{O}_{U_i}^{n_i}$ for some positive integer n_i. A *trivialisation* of $\mathcal{F}$ is a covering $\mathcal{U}$ as above and a system of isomorphisms $\mathcal{O}_{U_i}^{n_i} \cong \mathcal{F}|_{U_i}$.

If X is connected, then the n_i are all equal to the same number n called the *rank* of $\mathcal{F}$. A locally free sheaf of rank 1 is called an *invertible sheaf* or a *line bundle.*

Remark 4.2 For any locally free sheaf $\mathcal{F}$ and point $P \in X$ with residue field $\kappa(P)$ the group $\mathcal{F}_P \otimes \kappa(P)$ is a finite dimensional $\kappa(P)$-vector space. So we may think of a locally free sheaf as a family of $\kappa(P)$-vector spaces which is "locally trivial". In fact, locally free sheaves correspond to vector bundles in the algebro-geometric context, whence the name line bundle in rank 1.

Lemma 4.3 *Any locally free sheaf is coherent. Moreover, if X is noetherian and connected, a coherent sheaf $\mathcal{F}$ on X is locally free of rank n if and only if it stalk $\mathcal{F}_P$ at each point P is a free $\mathcal{O}_{X,P}$-module of rank n.*

Proof: For the first statement, take any affine open subset $V = \operatorname{Spec} A$ contained in one of the U_i as in the definition. Then by the assumption the restriction of $\mathcal{F}$ to V is isomorphic to the coherent sheaf defined by the free A-module $A \oplus \ldots \oplus A$ (with A repeated n_i times).

In the second statement necessity follows from the definitions by taking the direct limit. For sufficiency, assume $\mathcal{F}_P$ is freely generated over $\mathcal{O}_{X,P}$ by some generators $t_1, \ldots, t_n$. We may view the t_i as sections generating $\mathcal{F}(U)$

for some suficiently small open neighbourhood U of P. By shrinking U if necessary we may assume $U = \operatorname{Spec} A$ and $\mathcal{F} = \tilde{M}$ for some A-module M generated by the t_i. Since X is noetherian, M is the quotient of the free A-module of rank n by a submodule generated by *finitely many* relations among the t_i. By assumption, any of the finitely many coefficients occuring in these relations vanishes when restricted to some open neighbourhood of P contained in U. Denoting by V the intersection of these neighbourhoods, the elements $t_i|_V$ generate $\mathcal{F}|_V$ freely over $\mathcal{O}_V$. □

Remark 4.4 A similar (but easier) argument as in the second part of the above proof shows that if $\mathcal{F}$ is a coherent sheaf on any scheme X and P is a point for which $\mathcal{F}_P = 0$ then there is some open neighbourhood V of P with $\mathcal{F}|_V = 0$.

The crucial importance of invertible sheaves for the study of Dedekid schemes is shown by the following proposition.

Proposition 4.5 *Any nonzero coherent sheaf of ideals $\mathcal{I}$ on a Dedekind scheme X is invertible.*

Proof: By the criterion of Lemma 4.3, it is enough to check that $\mathcal{I}_P$ is a free $\mathcal{O}_{X,P}$-module of rank 1 for each $P \in X$. If P is the generic point, this is obviously true since any nonzero ideal in a ring generates the unit ideal in its fraction field. If P is a closed point, we are done by the fact that $\mathcal{O}_{X,P}$ is a principal ideal ring. □

Up to now, the notion of an invertible sheaf may well have seemed to be rather abstract, but now we explain a method for constructing invertible sheaves on Dedekind schemes. First a definition.

Definition 4.6 A *(Weil) divisor* on a Dedekind scheme X is an element of the free abelian group $Div(X)$ generated by the closed points of X.

Thus a divisor is just a formal linear combination $D = \sum m_i P_i$ of finitely many closed points of X. If P is a closed point, we define $v_P(D)$ to be equal to m_i if $P = P_i$ for some i and 0 otherwise. On the other hand, let K be the function field of X; it is the common fraction field of all local rings of X. Since the local ring $\mathcal{O}_{X,P}$ is a discrete valuation ring, there is an associated discrete valuation v_P on K which takes finite values on nonzero elements of K. By analogy with the case of meromorphic functions on a Riemann surface, for a nonzero element $f \neq 0$ of K we say that f has a *zero of order m at P* if $m = v_P(f) > 0$ and that f has a *pole of order m at P*

if $m = v_P(f) < 0$. The following lemma shows that elements of K behave in a similar way to meromorphic functions on a *compact* Riemann surface (compare with the proof of Chapter 4, Lemma 3.2):

Lemma 4.7 *If X is a Dedekind scheme with function field K, any nonzero function $f \in K$ has only finitely many zeros and poles.*

Proof: This follows from Chapter 5, Lemma **??** and the first statement of Proposition 2.16. □

Thanks to the lemma, we may define the *divisor* of a nonzero function $f \in K$ as the divisor D with $v_P(D) = v_P(f)$ for all closed points P. In this way, we obtain a homomorphism

$$div : K^{\times} \to Div(X)$$

where $K^{\times}$ is the multiplicative group of K. Elements of the image of div are traditionally called *principal divisors.*

Now denote by $\mathcal{K}$ the constant abelian sheaf on X defined by *the additive group* of K. It has an $\mathcal{O}_X$-module structure coming from the natural embedding of $\mathcal{O}_X$ into $\mathcal{K}$ but is not a quasi-coherent sheaf. However, given any divisor $D \in Div(X)$ we may define a subsheaf of $\mathcal{K}$ which is not only quasi-coherent but, as we shall see shortly, even invertible. Namely, define for any open subset $U \subset X$

$$\mathcal{L}(D)(U) := \{f \in \mathcal{K}(U) : v_P(f) + v_P(D) \geq 0 \text{ for all closed points } P \in U\}.$$

One sees immediately that together with the restriction maps induced by those of $\mathcal{K}$ we get a subsheaf $\mathcal{L}(D)$ of $\mathcal{K}$. One thinks of the sections of $\mathcal{L}(D)$ over U as functions with local behaviour determined by the "restriction of D to U": they should be regular except perhaps at the points $P \in U$ with $v_P(D) > 0$ where a pole of order at most $v_P(D)$ is allowed; furthermore, at points with $v_P(D) < 0$ they should have a zero of order at least $-v_P(D)$. Thus the sheaf $\mathcal{L}(0)$ is none but the image of $\mathcal{O}_X$ in $\mathcal{K}$ via the natural embedding. Moreover, each $\mathcal{L}(D)$ becomes an $\mathcal{O}_X$-submodule of $\mathcal{K}$ with its natural $\mathcal{O}_X$-module structure.

Proposition 4.8 *Each $\mathcal{L}(D)$ is an invertible sheaf on the Dedekind scheme X. Moreover the rule $D \mapsto \mathcal{L}(D)$ induces a bijection between divisors and invertible subsheaves of $\mathcal{K}$.*

Here the term "invertible subsheaf" means that we consider invertible sheaves which are $\mathcal{O}_X$-submodules of $\mathcal{K}$ with its canonical $\mathcal{O}_X$-module structure.

Proof: For the first statement, let P be a closed point of X and $f \in K^\times$ a function with $v_P(f) = v_P(D)$ (for example, a power of a generator of the maximal ideal of $\mathcal{O}_{X,P}$). Denote by S the set of closed points Q of X with $v_Q(D) \neq 0$ or $v_Q(f) \neq 0$. According to the previous lemma, S is a finite set. Now let U be the open set $(X \setminus S) \cup \{P\}$. Over U, the sections of $\mathcal{L}(D)$ are functions g which are regular outside P and $v_P(g) + v_P(f) \geq 0$. Hence the map of $\mathcal{O}_U$-modules induced by $1 \mapsto f^{-1}$ gives an isomorphism of $\mathcal{O}_U$ onto $\mathcal{L}(D)|_U$. Since P was arbitrary, we get a covering of X by open subsets over each of which $\mathcal{L}(D)$ is isomorphic to the structure sheaf.

Conversely, given an invertible subsheaf $\mathcal{L}$ of $\mathcal{K}$ there is a trivialisation of $\mathcal{L}$ over some open covering $\mathcal{U}$ which we may choose finite by compactness of X. For each $U_i \in \mathcal{U}$ denote by f_i the image of $1 \in \mathcal{O}_X(U_i)$ under the isomorphism $\mathcal{O}_X(U_i) \cong \mathcal{L}(U_i)$ arising from the trivialisation. Now define a divisor D by setting $v_P(D) = -v_P(f_i)$ where i is an integer for which $P \in U_i$. Since the finitely many f_i have finitely many zeros and poles according to the previous lemma, D is indeed a divisor. We still have to check that the definition of D does not depend on the choices made. First, if $P \in U_i \cap U_j$, viewing f_i and f_j as elements of $\mathcal{O}_{X,P}$ we see that there should exist functions $u, v \in \mathcal{O}_{X,P}$ with $f_i = uf_j$ and $f_j = vf_i$, whence both u and v are units in $\mathcal{O}_{X,P}$ and $v_P(f_i) = v_P(f_j)$. Secondly, the definition of D does not depend on the choice of the trivialisation for passing to another one induces an automorphism of the stalk $\mathcal{L}_P$ viewed as a free $\mathcal{O}_{X,P}$-module of rank 1, and such an automorphism is given by multiplication with a unit of $\mathcal{O}_{X,P}$. Finally, one checks by going through the above construction that $\mathcal{L} = \mathcal{L}(D)$. □

The proof shows that in the case when $v_P(D) \geq 0$ for all P the sheaf $\mathcal{L}(-D)$ is a subsheaf not only of $\mathcal{K}$ but also of $\mathcal{O}_X$ and hence is an ideal sheaf. Now assume $X = \operatorname{Spec} A$ is affine and take a nonzero ideal I of A. According to Proposition 4.5, the coherent ideal sheaf $\tilde{I}$ is an invertible subsheaf of $\mathcal{K}$, so the proposition applies and shows that $\tilde{I}$ can be identified with an invertible sheaf of the form $\mathcal{L}(-D)$, where $D = \sum m_i P_i$ is a divisor with all $m_i > 0$. By definition, a global section of the latter sheaf is an element of A contained in the intersection $\cap P_i^{m_i}$, where the P_i are viewed as prime ideals of A. But as the ideals $P_i^{m_i}$ are pairwise coprime, their intersection is the same as their product, so by taking global sections of $\tilde{I} = \mathcal{L}(-D)$ we get:

Corollary 4.9 *In a Dedekind ring any ideal decomposes uniquely as a product of prime ideals.*

This applies in particular to rings of integers in number fields. For the ring **Z** it is none but the Fundamental Theorem of Arithmetic.

Remark 4.10 Of course, we could have obtained this result without making all this *détour* amidst schemes and invertible sheaves. But having done so, we get as a bonus a geometric interpretation of the situation, namely that ideals in a Dedekind ring can be regarded as compatible systems of local solutions for a problem of finding functions with restricted behaviour at a finite set of points. This problem can be regarded as an analogue of the classical Mittag-Leffler and Weierstrass problems in complex analysis.

Remark 4.11 The preceding arguments also enable one to prove directly that on $X = \operatorname{Spec} A$ all quasi-coherent ideal sheaves (in fect, all of them are also coherent for A is noetherian) are isomorphic to some $\tilde{I}$. Indeed, we already know that nonzero ideal sheaves are of the form $\mathcal{L}(-D)$, with $v_P(D) \geq 0$ for all P; put $I = \mathcal{L}(-D)(X)$. By Chapter 4, Lemma 2.7 (3) and the sheaf axioms it is enough to show the existence of compatible isomorphisms $\mathcal{I}(U) \cong \mathcal{L}(-D)(U)$ over basic open sets $U = D(f)$. But we have $\tilde{I}(U) = I \otimes_A A_f$ and by the same argument as for $U = X$ we get $\mathcal{L}(D)(U) = IA_f$; the isomorphism is then given by the natural multiplication map $I \otimes_A A_f \to IA_f$.

Returning to Proposition 4.8, one might be under the impression that the invertible sheaves that are subsheaves of $\mathcal{K}$ (and hence arise from divisors) are rather special. This is a misbelief, for we have quite generally:

Proposition 4.12 *Let X be an integral scheme whose underlying topological space is compact. Then any invertible sheaf $\mathcal{L}$ on X is isomorphic to a subsheaf of the constant sheaf $\mathcal{K}$ associated to the function field of X.*

Proof: By compactness we may choose a trivialisation of $\mathcal{L}$ over a *finite* covering of X by open subsets $U_1, \ldots, U_n$; by irreducibility of X the intersection $U_0 = \cap U_i$ is a nonempty open subset in X. For each integer $0 \leq i \leq n$ let s_i be the image of 1 by the isomorphism $\mathcal{O}_X(U_i) \cong \mathcal{L}(U_i)$ coming from the chosen trivialisation. For each $i > 0$ there exists a section $f_i \in \mathcal{O}_X(U_0)$ with $f_i s_0 = s_i|_{U_0}$. Now we define an injective morphism $\mathcal{L} \to \mathcal{K}$. According to the third part of Chapter 4, Lemma 2.7 for this it is enough to define a compatible system of embeddings $\mathcal{L}(U) \to \mathcal{K}(U)$ over those open subsets U with $U \subset U_i$ for some i. These we define as the $\mathcal{O}_X(U)$-module homomorphisms induced by the maps $s_i|_U \to f_i|_U$, viewing f_i as a global section of $\mathcal{K}$. The definition does not depend on the choice of i, for if $U \subset U_i \cap U_j$ and $s \in \mathcal{L}(U)$ arises both as $s = a_i s_i|_U$ and $s = a_j s_j|_U$, we have $s|_{U_0} = a_i f_i s_0 = a_j f_j s_0$, whence the function $a_i f_i - a_j f_j$ vanishes over the dense open subset U, so $a_i f_i = a_j f_j$ in $K = \mathcal{K}(X)$ by Chapter 5, Lemma **??**. Injectivity of the morphisms $\mathcal{L}(U) \to \mathcal{K}(U)$ is obvious. □

Remark 4.13 In fact, the compactness assumption in the proposition is superfluous. See Hartshorne [1], Proposition II.6.15.

Next, note that Proposition 4.8 implies that over a Dedekind scheme it is possible to introduce an abelian group law on the set of invertible subsheaves of $\mathcal{K}$, by the rule $\mathcal{L}(D_1) \times \mathcal{L}(D_2) \to \mathcal{L}(D_1 + D_2)$ for any two divisors D_1, D_2. In this way the map $D \mapsto \mathcal{L}(D)$ becomes a group homomorphism.

But in view of the above proposition, it is interesting to know that one may define a natural abelian group law on the set of *isomorphism classes of* invertible sheaves on any scheme X. For this we first need the notion of the *tensor product* $\mathcal{F} \otimes \mathcal{G}$ of two $\mathcal{O}_X$-modules $\mathcal{F}$ and $\mathcal{G}$: this is none but the sheaf associated to the presheaf $U \to \mathcal{F}(U) \otimes_{\mathcal{O}_X(U)} \mathcal{G}(U)$.

Remark 4.14 One checks easily that $\mathcal{F} \otimes \mathcal{G}$ represents the set-valued functor on the category of $\mathcal{O}_X$-modules which maps an $\mathcal{O}_X$-module $\mathcal{M}$ to the set of $\mathcal{O}_X$-bilinear maps $\mathcal{F} \times \mathcal{G} \to \mathcal{M}$. (Use the representability for each U of the functor associating $\mathcal{O}_X(U)$-bilinear maps $\mathcal{F}(U) \times \mathcal{G}(U) \to \mathcal{M}(U)$ to $\mathcal{M}(U)$ and conclude by Chapter 3, Remark 2.9.)

Proposition 4.15 *For any scheme X, tensor product of $\mathcal{O}_X$-modules induces an abelian group structure on the set of isomorphism classes of invertible sheaves on X. The unit element of this group is $\mathcal{O}_X$ and the inverse of a class represented by an invertible sheaf $\mathcal{L}$ is the class of the sheaf $\mathcal{L}^\vee$ given by $U \to \mathrm{Hom}_{\mathcal{O}_U}(\mathcal{L}|_U, \mathcal{O}_U)$.*

For the proof we need two general lemmata.

Lemma 4.16 *If $\mathcal{F}$ and $\mathcal{G}$ are two $\mathcal{O}_X$-modules on a scheme X and P is a point of X, we have a natural isomorphism on the stalks*

$$(\mathcal{F} \otimes \mathcal{G})_P \cong \mathcal{F}_P \otimes_{\mathcal{O}_{X,P}} \mathcal{G}_P.$$

Proof: This follows by nasty checking from the definitions. Note that since the stalks of the sheaf associated to a presheaf are the same as that of the presheaf it is enough to work with the presheaf tensor product $U \to \mathcal{F}(U) \otimes_{\mathcal{O}_X(U)} \mathcal{G}(U)$. □

Lemma 4.17 *A morphism $\phi : \mathcal{F} \to \mathcal{G}$ of abelian sheaves on a topological space is an isomorphism if and only if for each point P the induced group homomorphisms on the stalks $\phi_P : \mathcal{F}_P \to \mathcal{G}_P$ are.*

Proof: One implication is easy. For the other, assume that the ϕ_P are all isomorphisms. We have to show that the maps $\phi_U : \mathcal{F}(U) \to \mathcal{G}(U)$ are all bijective. For injectivity, assume $s \in \mathcal{F}(U)$ maps to 0 by ϕ_U. Then by injectivity of the maps ϕ_P for $P \in U$ we get that the image of s in the stalks $\mathcal{F}_P$ is 0 for all P, whence a covering of U by open subsets over each of which s restricts to 0. Hence $s = 0$ by the first sheaf axiom. The proof of surjectivity is similar, using the second sheaf axiom (and the injectivity just proven). □

Proof of Proposition 4.15: The group law is well defined since the tensor product of modules respects isomorphisms. The abelian group axioms concerning commutativity, associativity and the unit element follow from the corresponding properties of the tensor product (of modules, which are clearly inherited by $\mathcal{O}_X$-modules). So only the axiom concerning the inverse remains. For each open set U define a morphism $\mathcal{L}(U) \times \mathrm{Hom}_{\mathcal{O}_X(U)}(\mathcal{L}(U), \mathcal{O}_X(U)) \to \mathcal{O}_X(U)$ by the natural evaluation map $(s, \phi) \mapsto \phi(s)$. This is clearly compatible with restriction maps for open inclusions $V \subset U$ and moreover it is $\mathcal{O}_X(U)$-bilinear, so it induces a morphism of $\mathcal{O}_X$-modules $\mathcal{L} \otimes \mathcal{L}^\vee \to \mathcal{O}_X$. To show that it is an isomorphism, it is enough to look at the induced maps $\mathcal{L}_P \otimes_{\mathcal{O}_{X,P}} \mathcal{L}_P^\vee \to \mathcal{O}_{X,P}$ on stalks by the previous two lemmata. But since $\mathcal{L}_P$ is a free $\mathcal{O}_{X,P}$-module of rank 1, we have isomorphisms

$$\mathcal{L}_P \otimes_{\mathcal{O}_{X,P}} \mathrm{Hom}_{\mathcal{O}_{X,P}}(\mathcal{L}_P, \mathcal{O}_{X,P}) \cong \mathcal{O}_{X,P} \otimes_{\mathcal{O}_{X,P}} \mathrm{Hom}_{\mathcal{O}_{X,P}}(\mathcal{O}_{X,P}, \mathcal{O}_{X,P}) \cong \mathcal{O}_{X,P}$$

and we are done.

Definition 4.18 The group of isomorphism classes of invertible sheaves on a scheme X is called the Picard group of X and is denoted by $Pic(X)$.

We finally establish the link between the group $Div(X)$ of divisors on a Dedekind scheme and the group $Pic(X)$. For this denote by $[\mathcal{L}]$ the class of an invertible sheaf $\mathcal{L}$ in the Picard group. By what we have seen so far, we dispose of a map $Div(X) \to Pic(X)$ given by $D \mapsto [\mathcal{L}(D)]$.

Lemma 4.19 *The above map $D \mapsto [\mathcal{L}(D)]$ is a group homomorphism.*

Proof: We have already seen that the map $D \mapsto \mathcal{L}(D)$ is a homomorphism. Recall that here the multiplication map $\mathcal{L}(D_1) \times \mathcal{L}(D_2) \to \mathcal{L}(D_1 + D_2)$ for two divisors D_1, D_2 is given by multiplication of functions. This map is $\mathcal{O}_X$-bilinear and as such induces a morphism of $\mathcal{O}_X$-modules $\mathcal{L}(D_1) \otimes \mathcal{L}(D_2) \to \mathcal{L}(D_1 + D_2)$. It is then enough to see that this latter map is an isomorphism, which can be checked on the stalks. The stalk of $\mathcal{L}(D_i)$ $(i = 1, 2)$ at a point P is a free $\mathcal{O}_{X,P}$-module generated by some f_i; that of $\mathcal{L}(D_1) \otimes \mathcal{L}(D_2)$ is generated by $f_1 \otimes f_2$ and that of $\mathcal{L}(D_1 + D_2)$ by $f_1 f_2$. Hence mapping $f_1 \otimes f_2$ to $f_1 f_2$ indeed induces an isomorphism. □

Proposition 4.20 *The sequence*

$$0 \to \mathcal{O}_X(X)^\times \to K^\times \xrightarrow{div} Div(X) \xrightarrow{D \mapsto [\mathcal{L}(D)]} Pic(X) \to 0$$

is exact, where $\mathcal{O}_X(X)^\times$ is the multiplicative group of units of $\mathcal{O}_X(X)$.

Proof: Exactness at the first two terms on the left is immediate from the definitions and surjectivity on the right follows from Propositions 4.8 and 4.12. For exactness at the third term note first that for any divisor of the form $D = div(f)$ the invertible sheaf $\mathcal{L}(D)$ maps to the unit element of the Picard group as multiplying sections of $\mathcal{L}(D)$ over an open set U by $f|_U$ induces an isomorphism $\mathcal{L}(D) \cong \mathcal{O}_X$. Conversely, if such an isomorphism is known, let f be the image of $1 \in \mathcal{O}_X(X)$ by this isomorphism. Then one checks easily that $D = div(f^{-1})$. □

Remarks 4.21

1. Traditionally when $X = \operatorname{Spec} A$, the cokernel of the map *div* is called the *(ideal) class group* of the Dedekind ring A. When A is the ring of integers in a number field, a classical theorem of the arithmetic of number fields asserts that this is a *finite*. See e.g. Lang [2], p. 100 or Neukirch [1], Chapter I, Theorem 6.3 for a proof of this fundamental fact.

2. The results of this section generalise to integral schemes that are *locally factorial*, i.e. their local rings are unique factorisation domains. In the general context closed points have to be replaced by closed subschemes of codimension one. See Hartshorne [1], Section II.6 for details.

Chapter 7

Finite Covers of Dedekind Schemes

In this chapter we study finite (branched) covers of Dedekind schemes, which will turn out to behave in a strongly analogous way to finite branched covers of compact Riemann surfaces. On the way, we also prove classical number-theoretic results in a geometric manner which emphasises their analogy with the theory of branched covers.

1. Local Behaviour of Finite Morphisms

We begin with some examples.

Example 1.1 Consider the ring $\mathbf{Z}[i]$ of Gaussian integers; this is the ring of integers of the algebraic number field $\mathbf{Q}(i)$. The natural inclusion corresponds to a morphism of Dedekind schemes $\operatorname{Spec}\mathbf{Z}[i] \to \operatorname{Spec}\mathbf{Z}$: we now describe its fibres.

The fibre over the generic point (0) is

$$\operatorname{Spec}(\mathbf{Z}[i] \otimes_{\mathbf{Z}} \mathbf{Q}) \cong \operatorname{Spec}((\mathbf{Z}[x]/(x^2+1)) \otimes_{\mathbf{Z}} \mathbf{Q}) \cong \operatorname{Spec}\mathbf{Q}[x]/(x^2+1) \cong \mathbf{Q}(i).$$

Similarly, the fibre over a closed point (p) of $\operatorname{Spec}\mathbf{Z}$ is $\operatorname{Spec}(\mathbf{Z}[i] \otimes_{\mathbf{Z}} \mathbf{F}_p) = \operatorname{Spec}(\mathbf{F}_p[x]/(x^2+1))$. Now there are three cases:

- If $p \equiv 1 \bmod 4$, then the polynomial x^2+1 factors as the product of two distinct linear terms over $\mathbf{F}_p$, hence (by the Chinese Remainder Theorem) the fibre is isomorphic to $\operatorname{Spec}(\mathbf{F}_p \oplus \mathbf{F}_p)$.
- If $p \equiv -1 \bmod 4$, then the polynomial x^2+1 is irreducible over $\mathbf{F}_p$ and hence the fibre is isomorphic to $\operatorname{Spec}\mathbf{F}_{p^2}$.
- For $p = 2$ we have $x^2+1 = (x+1)^2$ over $\mathbf{F}_p$ and hence the fibre is $\operatorname{Spec}(\mathbf{F}_p[x]/(x+1)^2)$. The underlying topological space of this scheme is a single point (the maximal ideal $(x+1)$) and the local ring at this point contains nilpotent elements (for example $x+1$).

One is thus tempted to regard the point in the fibre over $(2) \in \operatorname{Spec} \mathbf{Z}$ as a kind of a branch point for this is the only point contained in a fibre which is degenerate in the sense that there are nilpotent functions on it. (We shall see shortly that though the fibres of the second type consist only of a single point, it is not reasonable to consider them as degenerate.) The following example confirms this intuition.

Example 1.2 For Riemann surfaces, the basic example of a branched cover was the cover $\mathbf{C} \to \mathbf{C}$, $z \mapsto z^n$ (indeed, we saw that any branched cover is analytically isomorphic to this one in the neighbourhood of a branch point). Algebraically, this corresponds to the morphism $\operatorname{Spec} \mathbf{C}[z] \to \operatorname{Spec} \mathbf{C}[z]$ coming from the $\mathbf{C}$-algebra homomorphism $\mathbf{C}[z] \to \mathbf{C}[z]$ induced by $z \mapsto z^n$. Introduce the variable $y = z^n$ in the second ring: we thus have an isomorphism $\mathbf{C}[z] \cong \mathbf{C}[z,y]/(y - z^n)$ and the above homomorphism corresponds to mapping z to y. Now first look at the fibre over the generic point $(0) \in \operatorname{Spec} \mathbf{C}[z]$: it is

$$\operatorname{Spec} (\mathbf{C}[z,y]/(y - z^n) \otimes_{\mathbf{C}[z]} \mathbf{C}(z)) \cong \operatorname{Spec} (\mathbf{C}(y)[z]/(y - z^n))$$

(don't forget that the $\mathbf{C}[z]$-module structure on $\mathbf{C}[z,y]/(y - z^n)$ occuring in the tensor product is given by $z \mapsto y$). Hence the fibre is the spectrum of a degree n Galois field extension of the rational function field $\mathbf{C}(y)$.

Now a closed point of the Dedekind scheme $\operatorname{Spec} \mathbf{C}[z]$ is given by a maximal ideal $(z - a)$ with some $a \in \mathbf{C}$; the residue field of the local ring at this point is $\mathbf{C}[z]/(z - a) \cong \mathbf{C}$. Hence the fibre over this point is

$$\operatorname{Spec} (\mathbf{C}[z,y]/(y - z^n) \otimes_{\mathbf{C}[z]} \mathbf{C}) \cong \operatorname{Spec} (\mathbf{C}[z]/(a - z^n))$$

since the $\mathbf{C}[z]$-modules on the two terms of the tensor product are given respectively by $z \mapsto y$ and $z \mapsto a$. Now there are two cases:

- For $a \neq 0$ the polynomial $z^n - a$ splits into a product of n distinct linear terms over $\mathbf{C}$ and thus the fibre is $\operatorname{Spec} (\mathbf{C} \oplus \ldots \oplus \mathbf{C})$ (n copies).
- For $a = 0$ the fibre is $\operatorname{Spec} \mathbf{C}[z]/(z^n)$, a one-point scheme with nilpotent elements in its unique local ring.

Our intuition is thus confirmed and it can be made more precise: in the first two cases of the first example and in the first case of the second, the fibre is a *finite étale* k-scheme, whereas in the remaining cases of the two examples (the "branch points") it is not. This also explains why there were only two cases in the second example but three in the first: over $\mathbf{C}$ a finite étale algebra can only be a finite direct sum of copies of $\mathbf{C}$, whereas over a non-separably closed field we may have non-trivial finite separable field extensions as well.

The essence of the phenomenon encountered above is distilled in the definitions we are to give. First a natural restriction on morphisms which ensures in particular that they have finite fibres.

Definition 1.3 A morphism of schemes $\phi : Y \to X$ is called *finite* if X has a covering by open affine subsets $U_i = \operatorname{Spec} B_i$ such that for each i the open subscheme $V_i = \phi^{-1}(U_i)$ of Y is an affine scheme $V_i = \operatorname{Spec} A_i$ and the ring homomorphism $\lambda_i : A_i \to B_i$ corresponding to $\phi|_{V_i}$ turns B_i into a *finitely generated A_i-module.*

In particular, any finite morphism is affine. This implies that for any $P \in X$ the fibre Y_P is affine as well; the additional property of finite morphisms assures that Y_P is the spectrum of a finite dimensional $\kappa(P)$-algebra.

Remark 1.4 When we shall be dealing with a finite morphism $\phi : Y \to X$, with X a Dedekind scheme, we shall always assume that the induced map $\mathcal{O}_{X,\eta} \to (\phi_* \mathcal{O}_Y)_\eta$ at the generic point η of X is nonzero (and hence is an injection, for $\mathcal{O}_{X,\eta}$ is the function field of X). This seemingly innocent assumption has an important consequence (valid for any noetherian integral scheme in place of X): that the continuous map underlying ϕ is *surjective.* Indeed, if it were not, there would be a point $P \in X$ over which the fibre is vacuous, i.e. is the spectrum of the zero ring. But then by Nakayama's lemma (Chapter 6, Lemma 2.3), the stalk of $\phi_* \mathcal{O}_Y$ at P would be zero as well, so since $\phi_* \mathcal{O}_Y$ is a coherent sheaf, it would be 0 in an neighbourhood of P (by Chapter 6, Remark 4.4). But each such neighbourhood contains η, a contradiction.

Examples 1.5

1. If $K \subset L$ is an inclusion of number fields, then the induced morphism $\operatorname{Spec} O_L \to \operatorname{Spec} \mathcal{O}_K$ is finite as O_L is a finitely generated $\mathcal{O}_K$-module according to Chapter 6, Proposition 1.9.

2. We shall prove in the next chapter that any nonconstant morphism of smooth *projective* curves is finite. For affine plane curves, this is not always true: consider, for instance, the curve $\operatorname{Spec} \mathbf{C}[x, y]/(xy - 1) \cong \operatorname{Spec} \mathbf{C}[x, x^{-1}]$; this is the complex affine line with the point 0 removed. The natural inclusion map $\operatorname{Spec} \mathbf{C}[x, x^{-1}] \to \operatorname{Spec} \mathbf{C}[x]$ is not finite; it is not even surjective.

3. One may nevertheless construct many examples of finite maps of affine curves: for instance, $\operatorname{Spec}\mathbf{C}[x,y]/(y^n - f) \to \operatorname{Spec}\mathbf{C}[x]$ is such for any $f \in \mathbf{C}[x]$.

Remark 1.6 It can be shown that if $\phi : Y \to X$ is a finite morphism then *any* affine open cover of X satisfies the property of the definition. For basic open sets this is easy to check: if $D(f_i) = \operatorname{Spec}(A_i)_{f_i} \subset A_i$ is such, then the fact that B_i is a finitely generated A_i-module via λ_i immediately implies that $(B_i)_{\lambda_i(f_i)}$ is a finitely generated $(A_i)_{f_i}$-module.

We can now begin the analysis of fibres of finite morphisms. Given a finite morphism $\phi : Y \to X$, the fibre Y_P over any point P of X is the spectrum of a finite dimensional $\kappa(P)$-algebra, so by Chapter 5, Proposition 2.16 decomposes as a finite disjoint union of schemes each of which has a single point Q of X as its underlying space (a point in the topological fibre) such that all elements of the maximal ideal of the local ring at Q (i.e. the germs of functions vanishing at Q) are nilpotent.

Definition 1.7 Let X be a Dedekind scheme and $\phi : Y \to X$ a finite morphism. We say that ϕ is *étale at* a point $Q \in Y$ if the component of the fibre Y_P corresponding to Q is étale over $\operatorname{Spec}\kappa(P)$, i.e. if it is the spectrum of a finite separable field extension of $\kappa(P)$. The morphism ϕ is a *finite étale morphism* if it is étale at all points of Y.

In particular, all fibres of a finite étale morphism are finite étale schemes over residue fields of points of X.

Remark 1.8 Though not used explicitly in the above definition of finite étale morphisms, the assumption that X is a Dedekind scheme is important here. When defining finite étale morphisms of general schemes, one needs an additional assumption which is automatically satisfied here (see Chapter 9).

We can now state the main result of this section.

Theorem 1.9 *Let $\phi : Y \to X$ be a finite morphism of Dedekind schemes. Then ϕ is étale at a point Q of Y if and only if the stalk of the sheaf of relative differentials $\Omega_{Y/X}$ at Q is 0.*

Proof: Take an affine open neighbourhood $U = \operatorname{Spec} A$ of P whose inverse image in Y is of the form $V = \operatorname{Spec} B$ and identify P and Q with the corresponding prime ideals of B and A as usual. Then by the localisation property of differentials the stalk of $\Omega_{Y/X}$ at Q is $\Omega_{B_Q/A}$, with B_Q regarded as an A-algebra via the composite map $A \to B \to B_Q$.

Next observe that the local component of the fibre Y_P corresponding to Q is precisely $\operatorname{Spec}(B_Q \otimes_A \kappa(P))$. (Indeed, by definition the local component is the spectrum of the localisation $(B \otimes_A \kappa(P))_{\bar{Q}}$, where $\bar{Q}$ is the image of Q in $B \otimes_A \kappa(P)$. This localisation is obtained by localising first B/PB by the image of $(A/P) \setminus \{0\}$ and then by the complement of $\bar{Q}$ which is the same as localising B by Q first, then passing to the quotient by the image of P and finally localising by the image of $(A/P) \setminus \{0\}$.) By the base change property of differentials we have an isomorphism

$$\Omega_{(B_Q \otimes_A \kappa(P))/\kappa(P)} \cong \Omega_{B_Q/A} \otimes_{B_Q} (B_Q \otimes_A \kappa(P)).$$

Now assume $\Omega_{B_Q/A} = 0$. Then the left hand side vanishes and so by Chapter 6, Proposition 3.6 $B_Q \otimes_A \kappa(P)$ is étale over $\kappa(P)$, i.e. it is equal to $\kappa(Q)$ which is finite and separable over $\kappa(P)$. Conversely, if this is the case, then by applying the argument backwards we get that $\Omega_{B_Q/A} \otimes_{B_Q} \kappa(Q) \cong 0$. But this latter ring is isomorphic to $\Omega_{B_Q/A}/Q\Omega_{B_Q/A}$ and the assertion follows from Nakayama's lemma (Chapter 6, Lemma 2.3). □

Taking Chapter 6, Remark 4.4 into account, we get as a first corollary:

Corollary 1.10 *Let $\phi : Y \to X$ be a finite morphism of Dedekind schemes. Then the points of Y at which ϕ is étale form an open subset of Y. In particular, if the fibre of ϕ at the generic point is étale, then ϕ is étale at all but finitely many closed points of Y.*

Example 1.11 It may very well happen that the generic fibre is not étale and hence ϕ is nowhere étale. An example is given by the map $\operatorname{Spec} \mathbf{F}_p[t] \to \operatorname{Spec} \mathbf{F}_p[t]$ induced by the $\mathbf{F}_p$-algebra homomorphism $t \mapsto t^p$ (an analogue of Example 1.2 in characteristic $p > 0$). As already noted in Chapter 1, on the generic stalks this induces an inseparable field extension.

Remark 1.12 The theorem shows that when X and Y are smooth complex curves, then ϕ is étale precisely over those closed points $P \in X$ for which the associated holomorphic map gives a cover in some complex open neighbourhood of P. We illustrate this by the example when Y is an affine plane curve of equation $f(x, y) = 0$ and ϕ is the map which projects Y onto the x-axis;

the general case is based on the same principle. In our case $\Omega_{Y/X}$ is the coherent $\mathcal{O}_X$-module associated to the $\mathbf{C}[x,y]/(f)$-module with single generator dy and relation $\partial_y f$. Hence its stalk is 0 precisely at those points (x,y) of X where $\partial_y f(x,y) \neq 0$. But by the implicit function theorem, these are the points where the holomorphic map associated to ϕ is a local isomorphism; the points with $\partial_y f(x,y) = 0$ are the branch points.

We now introduce a useful concept originating in work of Dedekind.

Definition 1.13 Let $\phi : Y \to X$ be a finite morphism of Dedekind schemes which is étale at the generic point. Then the we define the *different* $\mathcal{D}_{Y/X}$ as the nonzero ideal sheaf on Y which is the annihilator of $\Omega_{Y/X}$.

Putting Theorem 1.9 together with the theory of the previous section we get:

Corollary 1.14 *For $\phi : Y \to X$ as in the above definition, the different $\mathcal{D}_{Y/X}$ is an invertible sheaf of the form $\mathcal{L}(D)$, where $D = \sum_i m_i Q_i$ is a divisor supported exactly at those points Q_i at which ϕ is not étale.*

Definition 1.15 The points Q_i arising in the above corollary are called the *branch points* of ϕ or those points at which ϕ is *ramified.*

Remark 1.16 In the case when $Y = \operatorname{Spec} O_L$ and $X = \operatorname{Spec} \mathcal{O}_K$ are spectra of rings of integers in number fields we get using Chapter 6, Remark 4.11 that the different is of the form $\tilde{I}$, with I an ideal of O_L. Thus I is a product of powers of those prime ideals of O_L at which the map is not étale. This gives the link to the classical concept of the different in algebraic number theory.

In the remaining of this section we investigate fibres of finite morphisms more closely, especially those containing branch points. For this the following observation is crucial.

Proposition 1.17 *Let $\phi : Y \to X$ be a finite morphism of Dedekind schemes, inducing a field extension $L|K$ on the generic stalks. Then $\phi_*\mathcal{O}_Y$ is a locally free $\mathcal{O}_X$-module of rank $|L : K|$.*

Proof: Let P be a point of X. As usual, we consider an affine open neighbourhood $U = \operatorname{Spec} A$ of P over which ϕ comes from a ring homomorphism $\lambda : A \to B$. Here B is the integral closure of A in L, being integrally closed and finite over A. Now the stalk of $\phi_*\mathcal{O}_Y$ at P is the spectrum of the A_P-algebra $B_P = B \otimes_A A_P$. This algebra can also be seen as the localisation of B by the multiplicatively closed subset $\lambda(A \setminus P)$. Indeed, given $f \in A \setminus P$, we have already seen in Chapter 6 during the construction of the sheaf of relative differentials that $B_{\lambda(f)}$ is canonically isomorphic to $B \otimes_A A_f$; the statement follows from this by passing to the direct limit (a union in this case). Taking Chapter 6, Lemma 1.8 into account, this shows that B_P is the integral closure of A_P in L. In particular, since any element of L can be multiplied with an appropriate element of K to become integral over A_P, any generating system of the finitely generated A_P-module B_P generates the K-vector space L. According to (the corollary to) Nakayama's lemma we get such a generating system by choosing elements $t_1, \dots, t_n \in B_P$ whose images modulo PB_P form a basis of the $\kappa(P)$-vector space B_P/PB_P (the spectrum of this $\kappa(P)$-algebra is none but the fibre over P). It remains to be seen that the t_i are linearly independent over K, for this implies $n = |L : K|$ as well. So assume there is a nontrivial relation $\sum a_i t_i = 0$ with $a_i \in K$. By multiplying with a suitable power of a generator of P (viewed as the maximal ideal of A_P) we may assume that all a_i lie in A_P and not all of them are in P. But then reducing modulo P we obtain a nontrivial relation among the t_i in B_P/PB_P, a contradiction. □

To derive the next result we need to introduce some notation and terminology. Recall that the fibre Y_P of ϕ over a point $P \in Y$ decomposes as a finite disjoint union of spectra of local $\kappa(P)$-algebras each of which corresponds to a point Q in the topological fibre. We have already seen during the proof of Theorem 1.9 that if $V = \operatorname{Spec} B$ is an affine open set containing Y_P, then the local component corresponding to Q is the spectrum of $B_Q \otimes_A \kappa(P) \cong B_Q/PB_Q$. Here B_Q is a discrete valuation ring whose maximal ideal QB_Q induces the maximal ideal $\bar{Q}$ of B_Q/PB_Q. By Chapter 5, Proposition 2.16 $\bar{Q}$ consists of nilpotent elements, so being finitely generated, it is actually a nilpotent ideal (i.e. some power of it is 0).

Definition 1.18 With the above notations, the smallest nonnegative integer n for which $\bar{Q}^n = 0$ is denoted by $e(Q|P)$ and is called the *ramification index* of ϕ at Q. The degree $f(Q|P)$ of the residue field extension $\kappa(Q)|\kappa(P)$ is called its *residue class degree.*

In particular, ϕ is étale at Q if and only if $e(Q|P) = 1$ and $\kappa(Q)$ is separable over $\kappa(P)$. In the case where $X = \operatorname{Spec} B$ and $Y = \operatorname{Spec} A$ are affine there is a more classical definition of the ramification index: it is the multiplicity of Q in the product decomposition of the ideal PB in B (cf. Chapter 6, Corollary 4.9).

Remark 1.19 Applying the above definition to Example 1.2 corroborates that the above definition of the ramification index is compatible with the one used for Riemann surfaces. The extension of non-trivial residue class degrees is, however, a phenomenon which does not arise over the complex numbers.

Now we can state a fundamental equality of the arithmetic of Dedekind schemes which is the analogue of Chapter 4, Proposition 2.5 (4).

Proposition 1.20 *In the situation of the previous proposition, let P be a point of Y. Then we have the equality*

$$\sum_Q e(Q|P)f(Q|P) = |L : K|$$

where Q runs over the points of the topological fibre over P.

Proof: During the previous proof we have seen that the dimension of the $\kappa(P)$-space B_P/PB_P is $|L : K|$. Since B_P/PB_P decomposes as a direct sum of its components B_Q/PB_Q it will be enough to show that the dimension of such a component over $\kappa(P)$ is precisely $e(Q|P)f(Q|P)$. For this, notice that since B_Q is a discrete valuation ring, multiplication by the k-th power of a generator of QB_Q induces an isomorphism $B_Q/QB_Q \cong (QB_Q)^k/(QB_Q)^{k+1}$ for any positive integer k. Hence (with notation as in the definition above) in the filtration

$$B_Q/PB_Q \supset \bar{Q} \supset \bar{Q}^2 \supset \ldots \supset \bar{Q}^{e(Q|P)} = 0$$

each successive quotient is isomorphic to $B_Q/QB_Q \cong \kappa(Q)$ and so is an $f(Q|P)$-dimensional $\kappa(P)$-vector space. This proves our claim. □

2. Fundamental Groups of Dedekind Schemes

In this section we shall construct a profinite group which classifies finite étale covers of a fixed Dedekind scheme just as the absolute Galois group classifies finite étale algebras over a field or as the profinite completion of the topological fundamental group classifies finite covers of a compact Riemann surface. The method we shall follow will be the exact analogue of the procedure for Riemann surfaces in Chapter 4, Section 3; the technical details will be different, though.

So to start the procedure, we have to study function fields of Dedekind schemes. Consider the functor which associates to a Dedekind scheme X its function field K. This is indeed a functor, for given another Dedekind scheme Y with function field L and a morphism $\phi : Y \to X$, we have an induced morphism $K \to L$ on generic stalks of structure sheaves. If the morphism ϕ is finite, we get in this way a finite field extension $L|K$. Call the morphism ϕ *separable* if the extension $L|K$ is separable.

Proposition 2.1 *Let X be a Dedekind scheme with function field K. Then for any finite separable extension $L|K$ there is a Dedekind scheme Y with function field L and equipped with a finite separable morphism $Y \to X$. Furthermore, the scheme Y is unique up to isomorphism (over X).*

The Dedekind scheme Y is called the *normalisation* of X in L.

Proof: First we prove uniqueness. Assume $\phi : Y \to X$ and $\phi' : Y' \to X$ are two normalisations of X in L. Choose some affine open subset $\operatorname{Spec} A \subset X$. By Remark 1.6, over any basic open set $D(f) = \operatorname{Spec} A_f \subset \operatorname{Spec} A$ both ϕ and ϕ' satisfy the condition for a finite map. Let $D(g)$ (resp. $D(g')$) be the basic open set in Y (resp. Y') which is the preimage of $D(f)$. Then both $\mathcal{O}_Y(D(g))$ and $\mathcal{O}_{Y'}(D(g'))$ are finitely generated A_f-modules. Moreover, they are integrally closed with fraction field L (since their localisations at closed points are), so they are both isomorphic to the integral closure of A_f in L via their embeddings in L. This yields an isomorphism $D(g) \cong D(g')$. Using Chapter 6, Lemma 1.8 we see that these isomorphisms are compatible over intersections of basic open sets, therefore they define an isomorphism of Y with Y' over X.

Now assume $X = \operatorname{Spec} A$ is affine with fraction field K and let B be the integral closure of A in L. To prove that $\operatorname{Spec} B$ is a Dedekind scheme one employs exactly the same argument as in the special case $A = \mathbf{Z}$ treated before in Chapter 6, Example 2.17 (note that it is here that we use separability of $L|K$). By Chapter 6, Proposition 1.9, B is a finitely generated A-module, so the morphism $\phi_A : \operatorname{Spec} B \to \operatorname{Spec} A$ is finite. Before going over to the general case, notice that if $U = \operatorname{Spec} A_f$ is a basic open subscheme of X, then Chapter 6, Lemma 1.8 implies that $\phi_A^{-1}(U)$ is the normalisation of U, for it is the spectrum of the localisation of B by $g = \phi_A^\sharp(f)$.

Now cover X with affine open subsets U_i. By the affine case, each U_i has a normalisation V_i equipped with a finite morphism $V_i \to U_i$. It will suffice to show that there exist isomorphisms $\phi_{ij} : \phi_i^{-1}(U_i \cap U_j) \to \phi_j^{-1}(U_i \cap U_j)$ compatible over triple intersections, for then the V_i may be patched together using the construction of Chapter 5, Construction 5.3. To do this, cover

$U_i \cap U_j$ by basic affine open sets W_k; their inverse images by ϕ_i and ϕ_j (which cover $\phi_i^{-1}(U_i \cap U_j)$ and $\phi_j^{-1}(U_i \cap U_j)$, respectively) both give a normalisation of W_k in L by the remark in the previous paragraph and hence are canonically isomorphic by the uniqueness statement. Since moreover these isomorphisms are readily seen to be compatible over the intersections of the W_k (which are themselves basic open sets), we can conclude that they can be patched together to define the required ϕ_{ij}: for the underlying continuous maps this is immediate and for the maps on the structure sheaves one uses the third part of Chapter 5, Lemma 2.7. □

For a fixed Dedekind scheme X define the category $\mathbf{Ded}_X^s$ of finite separable Dedekind schemes over X as the category whose objects are Dedekind schemes Y equipped with a finite separable morphism $Y \to X$ and whose morphisms are finite morphisms compatible with the projections onto X.

Corollary 2.2 *The functor mapping an object $Y \to X$ to the induced extension of function fields induces an anti-equivalence between the category $\mathbf{Ded}_X^s$ and the category of finite separable extensions of the function field K of X (with morphisms the inclusion maps).*

Proof: The proposition shows that the functor is essentially surjective; it remains to check that it is fully faithful. For this, note first that given a finite morphism $Y \to X$ inducing a finite separable extension $L|K$, there is an isomorphism of Y with the normalisation of X in L constructed in the above proof. Fixing such an isomorphism for each object of $\mathbf{Ded}_X^s$ we get a canonical bijection between morphisms $Y \to Z$ in $\mathbf{Ded}_X^s$ and morphisms between normalisations of X in finite separable extensions of K. But these in turn correspond bijectively to towers of extensions $K \subset L \subset M$ for the normalisation in M of the normalisation of X in L is none but the normalisation of X in M. □

Now let X be a Dedekind scheme. A *finite étale X-scheme* is a scheme Y equipped with a finite étale morphism $Y \to X$. The following result shows that such a Y can only be of a very special type.

Proposition 2.3 *Any finite étale X-scheme Y is a finite disjoint union of Dedekind schemes.*

Proof: Let Q be a closed point of Y and let B_Q be the local ring of Y at Q whose maximal ideal we also denote by Q. Denote by P the image of Q in X and by A_P its local ring, which is a discrete valuation ring with maximal ideal P generated by a single nonzero element t. The spectrum of $B_Q/PB_Q = B_Q/tB_Q$ is the local component of Q in the fibre over P, so it is a finite field extension of A/P by assumption. Hence t generates a maximal ideal in B_Q which is only possible for $Q = (t)$. Furthermore, B_Q is a noetherian local ring, being a localisation of a finitely generated A_P-module. We now show that B_Q is a discrete valuation ring. Combining what we know so far with Chapter 6, Lemma 2.2, it is enough to see that B is an integral domain. For this, let $M \in \operatorname{Spec} B_Q$ be an inverse image of the generic point (0) of $\operatorname{Spec} A_P$. Since M as an ideal of B_Q is properly contained in Q, we have $t \notin M$ and $m = bt$ for any $m \in M$ with some $b \in B_Q$. As M is a prime ideal, this forces $b \in M$, so that $QM = M$ and finally $M = 0$ by Nakayama's lemma.

Now since X is noetherian and Y is finite over X, we conclude from the definitions that Y is noetherian as well. Furthermore, now that we know that the local rings of Y at closed points are discrete valuation rings, we may conclude that Y is normal and of dimension 1 (since all other local rings are localisations of those at closed points). So it remains to be seen that Y is a finite disjoint union of integral schemes. For this, let $\eta_1, \dots, \eta_n$ be the finitely many points in the generic fibre Y_η and let Y_i be the closure of η_i in Y. We have $Y_i \neq Y_j$ for $i \neq j$ as the generic point of an irreducible closed subset is unique. But then the Y_i are pairwise disjoint, for if say Y_1 and Y_2 had a a closed point Q in common, then, since we may assume Y_1 not contained in Y_2, for an affine open subset $\operatorname{Spec} A \subset Y_1$ containing Q the irreducible closed subset $Y_2 \cap \operatorname{Spec} A \subset \operatorname{Spec} A$ would define a nonzero prime ideal of A properly contained in Q, which is impossible as the local ring at Q is a domain of dimension 1. Hence the Y_i are the finitely many connected components of Y; endowing them with their open subscheme structure we get a decomposition as required. □

Now if we wish to continue our program parallel to Chapter 4, Section 3, we need the following lemma.

Lemma 2.4 *Let $p : Y \to X$ be a finite morphism of Dedekind schemes.*

1. *$q : Z \to Y$ be a second finite morphism of Dedekind schemes. Then $p \circ q$ is étale if and only if p and q are étale.*

2. *Let now $q : Z \to X$ be a Dedekind scheme finite and étale over X. Then the morphism $Y \times_X Z \to Y$ is finite and étale and hence so is the composite $Y \times_X Z \to X$.*

Note that by our convention (Remark 1.4) all finite morphisms under consideration are surjective.

Proof: For the first statement, we may assume (using Remark 1.6 if necessary) that $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$, $Z = \operatorname{Spec} C$ are all affine. For a point $P \in \operatorname{Spec} A$ we have

$$C \otimes_A \kappa(P) \cong C \otimes_B B \otimes_A \kappa(P). \tag{7.1}$$

Now if $B \otimes_A \kappa(P)$ is a direct sum of finite separable extensions $\kappa(Q)|\kappa(P)$ and so is $C \otimes_B \kappa(Q)$ for each Q, we get that $C \otimes_A \kappa(P)$ is a direct sum of separable extensions. For the converse we argue as in the beginning of the proof of Chapter 4, Theorem 3.17: if $K \subset L \subset M$ are the respective function fields of X, Y and Z, it follows from Proposition 1.20 (in fact, already from Proposition **??**) that $C \otimes_A \kappa(P)$ is étale if and only if all of its residue fields are separable over $\kappa(P)$ and the sum of residue class degrees is $[M : K]$. Now if one of the residue fields of $B \otimes_A \kappa(P)$ is inseparable over $\kappa(P)$ or if the sum of its residue class degrees is less than $[L : K]$, then a counting shows that $C \otimes_A \kappa(P)$ cannot be étale. This not being the case by assumption, Y is étale over X, and since in this case by formula (7.1) $C \otimes_A \kappa(P)$ is just the direct sum of the $C \otimes_B \kappa(Q)$ for Q running over the points in the fibre Y_P, we see that $Z \to Y$ must be étale as well.

For the second statement, finiteness of the morphism $Y \times_X Z \to Y$ follows from the definitions. For étaleness again we may assume $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$, $Z = \operatorname{Spec} C$ are all affine. Then for $Q \in \operatorname{Spec} B$, we have

$$(B \otimes_A C) \otimes_B \kappa(Q) \cong C \otimes_A \kappa(Q).$$

But the homomorphism $A \to \kappa(Q)$ factors as $A \to \kappa(P) \to \kappa(Q)$, where P is the image of Q in X. Now since by assumption $C \otimes_A \kappa(P)$ is étale over $\kappa(P)$, the algebra $C \otimes_A \kappa(Q) \cong C \otimes_A \kappa(P) \otimes_{\kappa(P)} \kappa(Q)$ is étale over $\kappa(Q)$ (one may use Chapter 6, Proposition 3.6 and Lemma 3.5 (3)). □

Remark 2.5 It can be shown that if $p : Y \to X$ is a finite étale morphism of Dedekind schemes and $q : Z \to Y$ any morphism of Dedekind schemes such that the composite $p \circ q$ is finite and étale, then q is also finite and étale. This follows immediately from the first statement of the lemma and the definition of finite morphisms once we know that q is *surjective.* The proof of this innocent-looking fact, however, requires more technique than we have seen so far. We shall return to this point in Chapter 9.

Now let X be a Dedekind scheme with function field K and $\phi : Y \to X$ a Dedekind scheme finite and étale over X. By Proposition 2.3, the fibre of ϕ over the generic point of X is the spectrum of a finite étale K-algebra which defines via the functor of Chapter 1, Theorem 3.4 a finite continuous

Gal(K)-set S_Y. Moreover, the rule $Y \mapsto S_Y$ defines a functor from the category of schemes finite and étale over X to the category of finite continuous Gal(K)-sets. (The perceptive reader will have noticed that in order to make everything fit here we should consider only those morphisms between schemes over X which are finite and separable but if we admit the above remark this condition is satisfied by *all* morphisms of finite étale X-schemes.)

Theorem 2.6 *Let X be a Dedekind scheme with function field K. Fix a separable closure K^s of K and let K^{et} be the composite in K^s of all finite subextensions $L|K$ which correspond by Corollary 2.2 to Dedekind schemes étale over X. Then for each finite étale X-scheme $\phi : Y \to X$ the action of* Gal(K) *on the set S_Y defined above factors through the quotient* Gal$(K^{et}|K)$ *and in this way we obtain an equivalence between the category of schemes finite and étale over X and the category of finite continuous left* Gal$(K^{et}|K)$*-sets.*

To be consistent with the notations in previous chapters, we call the *opposite group* of Gal$(K^{et}|K)$ the *algebraic fundamental group* of the Dedekind scheme X.

Proof: The first statement of the theorem is immediate from the construction and implies via Chapter 1, Theorem 3.4 that the functor we are investigating is fully faithful. To see that any finite continuous Gal$(K^{et}|K)$-set S is isomorphic to some S_Y, one first produces from Chapter 1, Theorem 3.4 a finite direct sum of finite subextensions of $K^{et}|K$ giving rise to S. Then it remains to see that any finite subextension of $K^{et}|K$ is the function field of some Dedekind scheme finite and étale over X. But this can be proven by exactly the same argument as in the proof of Chapter 4, Theorem 3.17, using Lemma 2.4. □

Remark 2.7 We shall study of fundamental groups of smooth curves in the next section; here we briefly discuss spectra of rings of integers in number fields.

We know several classical facts concerning these from algebraic number theory. Firstly, a theorem of Minkowski states that $\pi_1(\mathrm{Spec}\,\mathbf{Z})$ is trivial. Secondly, a theorem of Hermite and Minkowski states that for any number field K the group $\pi_1(\mathrm{Spec}\,\mathcal{O}_K)$ has only finitely many finite quotients of given order. Thirdly, one of the main results of class field theory (usually attributed to Hilbert) states that the maximal abelian quotient of $\pi_1(\mathrm{Spec}\,\mathcal{O}_K)$ is finite for all K and isomorphic (up to a finite group of exponent 2 coming from so-called real places of K) to $Pic(\mathrm{Spec}\,\mathcal{O}_K)$ (see the next chapter for a geometric analogue). Proofs of these classical theorems can be found in the books of Lang [2] and Neukirch [1], for example.

But as for the groups $\pi_1(\operatorname{Spec} \mathcal{O}_K)$ themselves and not just their finite quotients, our current knowledge is far from being ample. For several structural results, including the fact that they are topologically finitely generated (in contrast to the groups $\operatorname{Gal}(K)$), see chapter X of the monograph of Neukirch-Schmidt-Wingberg [1], where the results are stated more generally for open subschemes of $\operatorname{Spec} \mathcal{O}_K$.

3. Galois Branched Covers and Henselisation

The perceptive reader has noted that though the main theorem of the last section was completely analogous to the topological situation, there was one point missing from the presentation, namely the analogue of Galois branched covers. In this section we first repair this sin of omission.

We define (rather tautologically) a finite morphism $\phi : Y \to X$ of Dedekind schemes to be *Galois* if the induced inclusion $K \subset L$ of function fields is a finite Galois extension. Now there is a natural action of the (finite) Galois group G on X defined as follows. Take an affine open covering of X by $U_i = \operatorname{Spec} A_i$ whose inverse image consists of affine open sets $V_i = \operatorname{Spec} B_i$. Then B is the integral closure of A_i in L, so that $\sigma(B_i) = B_i$ for all i and $\sigma \in G$ and if Q is a prime ideal in B_i, then $\sigma(Q)$ is also a prime ideal of B_i. From this we deduce an action of G on X as a topological space but we have actually more: from the automorphism $\sigma|_{B_i} : B_i \to B_i$ we deduce an automorphism of V_i by Chapter 5, Theorem 2.14. These automorphisms are easily seen to be compatible over the intersections $V_i \cap V_j$, so we get an action of G on X *as a scheme.*

The next proposition shows that topologically this action by G has the property of a Galois cover.

Proposition 3.1 *The group G acts transitively on the fibres of ϕ.*

Proof: We may assume $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$ are affine. Let P be a prime ideal of A and let Q_1 be a prime ideal of B with $Q_1 \cap A = P$. Let $Q_2, \dots, Q_r$ be the other prime ideals of B in the G-orbit of Q_1. Assume there is some prime ideal Q lying over P which is not among the Q_i. Since Q and the Q_i are all maximal ideals, we may apply the Chinese Remainder Theorem (Lang [1], Chapter II, Theorem 2.1) which gives an isomorphism $B/(QQ_1 \dots Q_r) \cong B/Q \oplus B/Q_1 \oplus \dots \oplus B/Q_r$, hence we may find $x \in Q$ not contained in any of the Q_i (we may even find an x mapping to 1 modulo each Q_i and to 0 modulo Q). Now for any $\sigma \in G$ the element $\sigma(x)$ is still outside each Q_i, hence the same holds for their product $N(x) = \prod_{\sigma \in G} \sigma(x)$. But $N(x) \in A$, which means that $N(x) \notin P$. But since $x \in Q$, we have $N(x) \in Q \cap A = P$, a contradiction. □

Remark 3.2 The proposition implies that X as a scheme is the quotient of Y by the action of G defined above. To make this precise, note that we may take the quotient of Y by the G-action in the category of locally ringed spaces just as in the construction of projective spaces: we take the quotient of the underlying space by the action of G, whence a canonical topological projection $p : Y \to Y/G$; then for each open set $U \subset Y/G$ we define $\mathcal{O}_{Y/G}(U)$ as the ring of G-invariant elements of $\mathcal{O}_Y(p^{-1}(U))$. One checks that $(Y/G, \mathcal{O}_{Y/G})$ is indeed a locally ringed space and there is a canonical map $\psi : Y/G \to X$ with $\phi = \psi \circ p$. By the proposition ψ is an isomorphism on the underlying topological spaces. Now observe that if we choose an affine open covering of X by subsets $\operatorname{Spec} A_i$ whose inverse images in Y are of the form $\operatorname{Spec} B_i$, then by construction the G-orbit of any point of Y is entirely contained in one of the $\operatorname{Spec} B_i$. This implies that we may define the structure of a scheme on Y/G by choosing as an affine open covering the schemes $\operatorname{Spec} B_i^G$, where B_i^G is the ring of G-invariant elements of B_i. By construction we have $B_i^G \cong A_i$ and hence $Y/G \cong X$ as schemes.

Now let us draw some immediate consequences from the proposition concerning the local behaviour of a morphism $\phi : Y \to X$ near branch points. Consider a point P of X and a point Q in the fibre over P. According to Proposition 3.1, any other point of the fibre Y_P over P is of the form $\sigma(Q)$ with some $\sigma \in G$ and by construction $e(\sigma(Q)|P) = e(Q|P)$ and $f(\sigma(Q)|P) = f(Q|P)$. Hence we may denote simply be e end f the common ramification index and residue class degree of the points in Y_P. Now let D_Q be the stabiliser of Q with respect to the action of G on Y. Again by Proposition 3.1, the cosets of G mod D_Q are in bijection with the points in Y_P. Hence Proposition 1.20 implies that the order of D_Q is exatly ef.

Now let L_Q be the fixed field of D_Q and X' the normalisation of X in L_Q. Denote by Q' the image of Q by the map $\phi' : Y \to X'$.

Lemma 3.3 *The topological fibre of ϕ' over Q' consists only of Q. We have the equalities*

$$e(Q|Q') = e, \quad f(Q|Q') = f \quad \text{and} \quad e(Q'|P) = f(Q'|P) = 1.$$

In particular, the finite morphism $X' \to X$ is étale at Q'.

Proof: According to Proposition 3.1, the group D_Q acts transitively on the fibre of ϕ' over Q'. On the other hand, it fixes Q, whence the first statement. The second statement follows from the already proven fact that the order of D_Q is ef in view of the equalities

$$e(Q|Q')e(Q'|P) = e \quad \text{and} \quad f(Q|Q')f(Q'|P) = f$$

which hold quite generally and follow from the definitions. □

Remark 3.4 In arithmetic terminology, the group D_Q is called the *decomposition group* of Q and L_Q is called its *decomposition field.*

Thus the local ring $\mathcal{O}_{X',Q}$ of X' at Q has the property that its integral closure in L is a discrete valuation ring (the local ring of Q) and hence the ramification index and the residue class degree are easy to compute; in particular, the formula of Proposition 1.20 reduces to $ef = [L : L_Q]$. This property is not shared by the local ring $\mathcal{O}_{X,P}$ of X at P: its integral closure in L has several maximal ideals corresponding to the points in the fibre Y_Q. We may of course localise at one of these to get an extension of discrete valuation rings but then we lose the finiteness property of the corresponding morphism of affine schemes.

So we see that in order to study the local behaviour of ϕ at Q it is much better to work with $\mathcal{O}_{X',Q}$ than with $\mathcal{O}_{X,P}$; moreover, by the corollary we get the same ramification index and residue class degree. This procedure is *a priori* only available in the Galois case but if $\phi : Y \to X$ is only seperable with function field extension $L|K$, we may embed L into a Galois extension M of K and study the corresponding morphism of Dedekind schemes. This prompts the idea that if we choose M to be the biggest Galois extension available, namely the separable closure, then by the generalising the above procedure we may reduce the study of the local behaviour of finite morphisms near branch points to a problem about finite extensions of discrete valuation rings.

We now make this idea precise. First an easy lemma which could have figured earlier.

Lemma 3.5 *Let A be a discrete valuation ring with maximal ideal P and B an integral extension of A. Then there is a prime ideal Q of B with $Q \cap A = P$.*

Note that here the morphism $\operatorname{Spec} B \to \operatorname{Spec} A$ is *not* assumed to be finite.

Proof: It is enough to show that $PB \neq B$, for then PB is contained in some maximal ideal of B whose intersection with B is nonzero according to Chapter 6, Lemma 1.5 (1) and hence cannot be but P. So assume $PB = B$. Then there are $b_1, \ldots, b_r \in B$ and $p_1, \ldots, p_r \in P$ with $\sum_i p_i b_i = 1$. Hence the subring $B' = A[b_1, \ldots, b_r]$ also satisfies $PB' = B'$. But B' is integral over A and hence a finitely generated A-module, so Nakayama's lemma implies $B' = 0$ which is absurd. □

Now we can generalise the situation of Corollary 3.3 above.

Construction 3.6 Let A be a discrete valuation ring with maximal ideal P and fraction field K. Fix a separable closure K^s of K. Denoting by B the integral closure of A in K^s, apply the lemma to find some $Q \in \operatorname{Spec} B$ lying above P. Let D_Q be the stabiliser of Q with respect to the natural action of $\mathrm{Gal}\,(K)$ on $\operatorname{Spec} B$ (defined in the same way as for finite Galois extensions). Let K' be the fixed field of D_Q and put $B' = B \cap K'$, $Q' = Q \cap B'$. The localisation of B' at Q' is called the *henselisation* of A and is denoted by A^h.

Proposition 3.7 *Let A, P, A^h, Q be as above.*

1. *The ring A^h is a discrete valuation ring with the same residue field as A. Its maximal ideal is generated by any generator of P.*
2. *The isomorphism class of A^h does not depend on the choice of the prime ideal Q.*

For the proof we need the following generalisation to Proposition 3.1 to infinite Galois extensions.

Lemma 3.8 *With notations as in the above construction, the group* $\mathrm{Gal}\,(K)$ *acts transitively on the maximal ideals of B lying over P.*

Proof: Take two such maximal ideals $Q_1 \neq Q_2$ and for each finite Galois subextension $L|K$ denote by $\mathcal{X}_L$ the set of those elements of $G = \mathrm{Gal}\,(K)$ which when restricted to L map $Q_1 \cap L$ onto $Q_2 \cap L$. Since the latter are prime ideals of the integral closure of A in L, Proposition 3.1 implies that $\mathcal{X}_L \neq \emptyset$ for any L. Moreover, each X_L is a closed subset of G, for if some $\sigma \notin X_L$, then the whole left coset $\sigma\mathrm{Gal}\,(L)$ of the open subgroup $\mathrm{Gal}\,(L)$ is contained in $G \setminus \mathcal{X}_L$. But G is compact, so we have $\mathcal{X} = \bigcap_L \mathcal{X}_L \neq \emptyset$. Any element of $\mathcal{X}$ maps Q_1 onto Q_2. □

Proof of Proposition 3.7: For the first statement, note that by Corollary 3.3 for any finite separable extension $L|K$ the ring $A^h \cap L$ is a discrete valuation ring whose spectrum is étale over $\operatorname{Spec} A$. Hence A^h is the union of an increasing chain of such discrete valuation rings, which shows that it is local (its maximal ideal being the union of that of the $L \cap A^h$, and the same holding for its units) and its maximal ideal is generated by any generator of P. The same type of argument shows that the residue field of A^h is the same of that of A. The second statement follows from the lemma which implies that performing the above construction with a maximal ideal above P other than Q yields the ring $\sigma(A^h)$ for some $\sigma \in \mathrm{Gal}\,(K)$. □

We conclude this section by the following proposition which shows that henselisations do serve for the purpose they were constructed for.

Proposition 3.9 *Let $Y \to X$ be a finite separable morphism of Dedekind schemes. Let L (resp. K) be the function field of Y (resp. of X), and embed $L|K$ into a separable closure $K^s|K$. Fix a closed point Q of Y mapping to a point P of X. Let $A_P = \mathcal{O}_{X,P}$ be the local ring of X at P and $B_Q = \mathcal{O}_{Y,Q}$ that of Y at Q. Finally, fix a henselisation A_P^h of A_P, with fraction field $K^h \subset K^s$.*

1. *The integral closure of A_P^h in the composite field LK^h is isomorphic to the henselisation B_Q^h of B_Q.*
2. *The finite map $\mathrm{Spec}\, B_Q^h \to \mathrm{Spec}\, A_P^h$ thus obtained has ramification index $e(Q|P)$ and residue class degree $f(Q|P)$.*
3. *The stalk of the different $D_{\mathrm{Spec}\, B_Q^h/\mathrm{Spec}\, A_P^h}$ of the above map at the closed point of $\mathrm{Spec}\, B_Q^h$ is the ideal of B_Q^h generated by the stalk of the different $\mathcal{D}_{Y/X}$ at Q. (Here B_Q is viewed as a subring of B_Q^h.)*

Proof: For the first statement, note that by construction B_Q^h is a discrete valuation ring with fraction field LK^h integral over A_P^h. The second statement follows from Corollary 3.3 by taking the intersection of LK^h with each finite Galois extension of K containing L. For the proof of the third statement, take an affine open neighbourhood $\mathrm{Spec}\, A$ of P with inverse image $\mathrm{Spec}\, B$ in Y. Then the stalk of $D_{Y/X}$ at Q is the annihilator of $\Omega_{B_Q/A} \cong \Omega_{B/A} \otimes_B B_Q$ by the localisation property of differentials, whereas $D_{\mathrm{Spec}\, B_Q^h/\mathrm{Spec}\, A_P^h}$ is the annihilator of $\Omega_{B_Q^h/A_P^h} \cong \Omega_{B/A} \otimes_A A_P^h$ by the first statement and the localisation property of differentials. □

4. Henselian Discrete Valuation Rings

By the results of the previous section, the study of the local behaviour of finite morphisms of Dedekind schemes can be reduced to the study of the induced morphisms on the henselisations. In this section we study the henselisations in general and determine their fundamental groups. First a general definition.

Definition 4.1 A discrete valuation ring is called *henselian* if its integral closure in any finite extension of its fraction field is a discrete valuation ring.

Remarks 4.2

1. This definition is in accordance with the classical definition of henselian valuations as in Neukirch [1]. For its relation to the more general concept of henselian local rings, see Remark 4.8 below.
2. An immediate consequence of the definition is that the integral closure of a henselian discrete valuation ring in any finite extension of its fraction field is again henselian.

The following proposition shows that the above definition is not out of place here.

Proposition 4.3 *The henselisation A^h of any discrete valuation ring A is henselian.*

Before the proof we recall a well-known algebraic lemma.

Lemma 4.4 *Let $L|K$ be a finite extension of fields of characteristic $p > 0$ and let $K \subset L' \subset L$ be the maximal separable subextension (i.e. the compositum of all separable extensions of K contained in L). Then there exists a positive integer m such that $x^{p^m} \in L'$ for all $x \in L$.*

For a proof, see Lang [1], Chapter V, Section 6. The extension $L|L'$ is called *purely inseparable.* We now have the following general lemma.

Lemma 4.5 *Let A be a discrete valuation ring with fraction field K of characteristic $p > 0$ and let L be a purely inseparable finite extension of K. Then the integral closure B of A in L is a discrete valuation ring.*

Proof: Let m be a positive integer for which $x^{p^m} \in K$ for all $x \in L$. Then if v denotes the discrete valuation associated to A, the map $x \mapsto v(x^{p^m})$ is a homomorphism from the multiplicative group of L to $\mathbf{Z}$. Moreover, denoting by b a positive generator of its image in $\mathbf{Z}$ and setting $w(0) = \infty$, the formula $w(x) = (1/b)v(x^{p^m})$ defines a discrete valuation $w : L \to \mathbf{Z} \cup \{\infty\}$. The valuation ring of w is precisely B, for an element $x \in L$ is integral over A if and only if $x^{p^m} \in A$. (Indeed, x^{p^m} is always an element of K and is integral over A if and only if x is; now use the fact that A is integrally closed.) □

Remark 4.6 Quite generally, the integral closure B of any integrally closed local domain A in a finite purely inseparable extension $L|K$ of its fraction field is always local. To see this, one shows that the elements $x \in L$ such that x^{p^m} lies in the maximal ideal of A form a unique maximal ideal in B.

Proof of Proposition 4.3: Let $L|K^h$ be a finite extension. The construction of A^h (and the arguments preceding it) imply that the integral closure A' of A^h in the maximal separable subextension $L' \subset L$ is a discrete valuation ring. The proposition then follows by applying the above lemma with L' in place of K and A' in place of A. □

Now we have the following important characterisation of henselian discrete valuation rings.

Proposition 4.7 *Let A be a discrete valuation ring with maximal ideal P. Then the following are equivalent:*

1. *A is henselian.*
2. *Any integral domain $B \supset A$ finitely generated as an A-module is a local ring.*
3. *Given a monic polynomial $f \in A[x]$ whose reduction $\bar{f}$ modulo P factors as $\bar{f} = \bar{f}_1\bar{f}_2$ with $\bar{f}_1$ and $\bar{f}_2$ relatively prime monic polynomials in $\kappa(P)[x]$, there exists a factorisation $f = f_1 f_2$ of f into the product of two relatively prime monic polynomials in $A[x]$ such that $\bar{f}_i = f_i$ modulo P for $i = 1, 2$.*
4. *If $f \in A[x]$ is a monic polynomial such that its reduction $\bar{f}$ modulo P has a* simple *root $\bar{\alpha}$ in $\kappa(P)$, then there is $\alpha \in A$ with $f(\alpha) = 0$ and $\bar{\alpha} = \alpha$ modulo P.*

Proof: To show that (1) implies (2), assume there is an integral domain $B \supset A$ with fraction field L that is finitely generated over A and has at least two maximal ideals $P_1 \neq P_2$. But then the common integral closure C of A and B in L has two different prime ideals lying above the P_i in contradiction with (1). This follows by applying Lemma 3.5 to the localisations of B (resp. C) at the P_i in place of the A (resp. B) that figures in the lemma.

Now suppose that A satisfies (2) but some monic polynomial $f \in A[x]$ provides a counterexample to the property (3). We may assume f is irreducible in $A[x]$ for otherwise an irreducible factor would still give a counterexample. This implies that (f) is a prime ideal of A, for A is a unique factorisation domain (in fact, to see this it would suffice to use that A is interally closed), and so $B = A[x]/(f)$ is an integral domain integral over A. But then by assumption

$$B/PB \cong B \otimes_A \kappa(P) \cong \kappa(P)[x]/(\bar{f}_1) + \kappa(P)[x]/(\bar{f}_2),$$

so B is not local.

Since (4) is just a special case of (3), it remains to prove that (4) implies (1) for which we employ an argument from Nagata [1]. Assume that the integral closure B of A in some finite extension $L|K$ has at least two distinct maximal ideals Q_1 and Q_2. We then concoct a polynomial $f \in A[x]$ which is a counterexample to (4). Thanks to Lemma 4.5 there is no harm in supposing $L|K$ separable and even Galois. Denote by H_1 the stabiliser of Q_1 in $G = \mathrm{Gal}\,(L|K)$, by L_1 its fixed field and by B' the integral closure of A in L_1. Let $1 = \sigma_1, \dots, \sigma_n$ be a system of *two-sided* representatives of G modulo H_1. We know from Proposition 3.1 that there are exactly n maximal ideals of B, namely $Q_i = \sigma_i(Q_1)$. Denote by Q'_i the image of each Q_i in $\mathrm{Spec}\,B'$; by Lemma 3.3 we have $Q'_i \neq Q'_1$ for any $i \neq 1$. Using the Chinese Remainder Theorem as in the proof of Proposition 3.1 we may thus find an element α lying in the intersection of the Q'_i for $i > 1$ but not in Q'_1 (and hence not in K). Since $\alpha \in L_1$, the $\sigma_i(\alpha)$ for $1 \leq i \leq n$ are exactly the distinct conjugates of α in L. Again using Proposition 3.1 and the fact that the σ_i form a two-sided system of representatives we may find for each $i \neq 1$ some $Q_j \neq Q_1$ with $\sigma_i(Q_j) = Q_1$. Thus $\sigma_i(\alpha) \in Q_1$ if and only if $i \neq 1$. Now look at the minimal polynomial $f = x^n + a_{n-1}x^{n-1} + \dots a_0 \in A[x]$ of α over K. Here a_{n-1} is up to sign the sum of the $\sigma_i(\alpha)$, so it does not lie in $Q_1 \cap A = P$. But for $s < n-1$ the coefficient a_s is (still up to sign) a higher order symmetric polynomial of the $\sigma_i(\alpha)$ and hence already lies in P. Thus by reducing $-a_{n-1}$ modulo P we get a simple root of $\bar{f} = x^n + \bar{a}_{n-1}x^{n-1}$. This contradicts (4) as f is irreducible over K. □

Remark 4.8 An analysis of the above proof shows that in proving the equivalence of statements (2)–(4) we did not use the assumption that A was noetherian of dimension 1, hence these are equivalent conditions for any integrally closed local domain. The construction of the henselisation also works in this generality. It gives an integrally closed local domain A^h with the same residue field as A and equipped with a local homomorphism $A \to A^h$. Moreover, A^h is seen to satisfy condition (2) above (and *a fortiori* (3), (4)).

In general one calls *any* local ring satisfying condition (3) a *henselian local ring*. It can then be shown (see Nagata [1], Theorem 4.11.7) that the henselisation A^h of an integrally closed local domain A represents the contravariant functor on the category of henselian local rings which associates to an object B the set of local homomorphisms $A \to B$. Thus A^h is the "smallest" henselian local ring equipped with a *local* homomorphism $A \to A^h$. In fact, if we take the above representability as the definition of the henselisation, then A^h can be shown to exist for any local ring A but then one has to use a different construction. See Milne [1], Section I.4 for more details concerning this point.

Example 4.9 Besides the henselisation, there is a classical example for a henselian discrete valuation ring, namely that of a *complete* discrete valuation ring which we now explain.

Quite generally, one calls a local ring A complete if the natural map $A \to \hat{A}$ into its completion (see Chapter 6, Remark **??**) is an isomorphism. Obviously $\hat{A}$ is complete for any local ring A, so as concrete examples we may mention the ring $\mathbf{Z}_p$ of p-adic integers encountered in Chapter 1 (which is the completion of the localisation of $\mathbf{Z}$ at (p)) and the ring of formal power series $k[[t]]$ over a field k (which is the completion of any discrete valuation ring with residue field k that contains a subring isomorphic to k).

Now we show that any complete local ring A satisfies condition (4) of Proposition 4.7; this assertion is classically known as Hensel's lemma, whence the term "henselian". So let P be the maximal ideal of A and assume the reduction $\bar{f}$ of $f \in A[x]$ modulo P has a root $a_1 \in A/P$ which is simple, i.e. $\bar{f}'(a_1) \neq 0$. We construct a lifting $a \in A$ of a_1 with $f(a) = 0$ by Newton's method of successive approximation. Represent a by a coherent sequence (a_i), with $a_i \in A/P^i$ and assume a_i is already determined (this being the case for $i = 1$). Lift a_i arbitrarily to an element $b_i \in A/P^{i+1}$; the a_{i+1} we are looking for must then be of the form $a_{i+1} = b_i + p$, with $p \in P^i/P^{i+1}$. Keeping the notation f for the image of f in $(A/P^{i+1})[x]$, the element $f'(b_i)$ is a unit in the local ring A/P^{i+1} for its image $f'(a_1)$ modulo P is nonzero. By the Taylor Formula of order 2 (which is quite formal for polynomials), we have

$$f(b_i + p) = f(b_i) + f'(b_i)p + cp^2$$

with some $c \in A/P^{i+1}$, but anyway we have $p^2 = 0$, so since we are aiming at $f(b_i + p) = 0$, we only have to choose $p = -f(b_i)/f'(b_i)$.

The next proposition shows that finite étale covers of spectra of henselian discrete valuation rings have a simple description.

Proposition 4.10 *Let $X = \operatorname{Spec} A$, where A is a henselian discrete valuation ring with maximal ideal P.*

1. *Let f be a polynomial whose reduction $\bar{f}$ modulo P is irreducible and defines a finite separable extension of $\kappa(P)$. Then the ring $B = A[x]/(f)$ is a discrete valuation ring and the canonical morphism $\operatorname{Spec} B \to X$ is finite and étale.*

2. *Any finite étale X-scheme is a finite disjoint union of affine schemes* $\operatorname{Spec} B$*, with B of the above type.*

3. *The functor* $\operatorname{Spec} B \mapsto \operatorname{Spec}(B \otimes_A \kappa(P))$ *defines an equivalence between the category of finite étale X-schemes and that of finite étale $\kappa(P)$-schemes.*

Proof: For the first statement, note that B is finitely generated as an A-module, and hence is noetherian. Since f is irreducible it is also an integral domain (see the proof of Proposition 4.7), and hence it is a local ring by Proposition 4.7 (2). By Chapter 6, Proposition 3.4, $\Omega_{B/A} = 0$ and so by base change $\Omega_{B \otimes_A \kappa(P)/\kappa(P)} = 0$, hence $\operatorname{Spec} B$ is étale over X and P generates the maximal ideal of B which is thus principal, so B is a discrete valuation ring.

For the second statement, note first that since the only affine covering of X is by X itself, any finite X-scheme is necessarily affine. If it is moreover étale, decomposing it into a finite disjoint union of components, we may assume it is integral and hence the spectrum of some integral domain B. By exactly the same argument as above, we see that B is a discrete valuation ring. Now to prove that B is of the required form, let $\bar{f}$ be the minimal polynomial of a generator $\bar{\alpha}$ of the separable field extension $B \otimes_A \kappa(P)|\kappa(P)$ and lift $\bar{f}$ to a polynomial $f \in A[x]$. By proposition 4.7 (4), $\bar{\alpha}$ lifts to a root of f in A, whence an injective morphism $A[x]/(f) \to B$. Here both rings are discrete valuation rings with the same residue field and their spectra are finite and étale over X, so by Proposition 1.20 their fraction field K must be the same. Thus both rings are equal to the integral closure of A in K.

In the last statement essential surjectivity follows if we show that any finite separable extension $L|\kappa(P)$ is the residue field of some extension $A[x]/(f)$ as in (1). For this we only have to take as f some lifting in $A[x]$ of the minimal polynomial of a generator of $L|\kappa(P)$. For fully faithfulness, assume $B = A[x]/(f)$, $C = A[x]/(g)$ are such that $\operatorname{Spec} B$, $\operatorname{Spec} C$ are étale over X and assume given a morphism $B \otimes_A \kappa(P) \to C \otimes_A \kappa(P)$. It is given by mapping a generator of the field extension $B \otimes_A \kappa(P)|\kappa(P)$ to a root $\bar{\alpha}$ of $\bar{f}$ in $C \otimes_A \kappa(P)$. Lifting $\bar{\alpha}$ to a root α of f in C gives a homomorphism $B \to C$ inducing the above one by tensoring with $\kappa(P)$. To see that this morphism is unique, it is enough to see that α is the unique root of f in C lifting $\bar{\alpha}$. For this, by enlarging C if necessary we may assume that $C \otimes_A \kappa(P)$ is Galois over $\kappa(P)$ (embed $C \otimes_A \kappa(P)|\kappa(P)$ in a finite Galois extension and lift its defining polynomial to $A[x]$). Then $\bar{f}$ decomposes as a product of distinct linear factors in $C \otimes_A \kappa(P)$ and each of its roots lifts to a different root of f in C. □

Corollary 4.11 *For X as in the proposition there is a canonical isomorphism $\pi_1(X)^{op} \cong \mathrm{Gal}\,(\kappa(P))$.*

Proof: The group $\pi_1(X)^{op}$ is the Galois group of the Galois extension $K^{et}|K$ defined in Theorem 2.6. Let A^{et} be the integral closure of A in K^{et}; as A is henselian, it is a local ring with maximal ideal P^{et}. Any element of $\mathrm{Gal}\,(K^{et}|K)$ maps A^{et} and P^{et} onto themselves and hence defines a $\kappa(P)$-automorphism of the field A^{et}/P^{et} which is none but a separable closure of $\kappa(P)$ by the third statement of the proposition. Whence a homomorphism $\pi_1(X)^{op} \to \mathrm{Gal}\,(\kappa(P))$ of which the proposition implies the bijectivity. □

Remark 4.12 Let $X = \mathrm{Spec}\, A$ be as above, and denote by K the fraction field of A. In this case the closed normal subgroup of $\mathrm{Gal}\,(K)$ which is the kernel of the canonical map $\mathrm{Gal}\,(K) \to \mathrm{Gal}\,(K^{et}|K)$ (and hence of the map $\mathrm{Gal}\,(K) \to \mathrm{Gal}\,(\kappa(P))$ defined by composing with the above isomorphism) is usually called the *inertia subgroup*.

5. Dedekind's Different Formula

In this section we harvest the fruits of our efforts in the two previous ones and complete our study of finite morphisms of Dedekind schemes; in particular we prove a classical formula of Dedekind computing the different.

First an easy application of the ideas we have just seen.

Proposition 5.1 *Let A be a henselian discrete valuation ring with fraction field K and maximal ideal P, let B be its integral closure in a finite separable extension $L|K$ and let Q be the maximal ideal of B. Assume further that the residual extension $\kappa(Q)|\kappa(P)$ is separable.*

Then there is a unique discrete valuation ring $A \subset C \subset B$ with residue field $\kappa(Q)$ and such that the map $\mathrm{Spec}\, C \to \mathrm{Spec}\, A$ is étale.

Proof: Embed L in a separable closure K^s and put $M = L \cap K^{et}$, with K^{et} as in Theorem 2.6. Let C be the integral closure of A in M. The affine scheme $\mathrm{Spec}\, C$ is integral, finite and étale over $\mathrm{Spec}\, A$ by construction and hence C is a discrete valuation ring by Proposition 4.10 (2). The residue field of C is $\kappa(Q)$, for otherwise, B being henselian by Remark 4.2 (2), arguing as in the proof of Proposition 4.10 (2) we would get a subring $C' \subset B$ properly containing C with residue field $\kappa(Q)$ and $\mathrm{Spec}\, C' \to \mathrm{Spec}\, A$ étale, contradicting the construction of C. □

Using Proposition 1.20 we get that in the situation of the proposition the finite morphism $\operatorname{Spec} B \to \operatorname{Spec} C$ has ramification index $e(Q|P)$ at Q and residue class degree 1. It is convenient to separate this property in a definition.

Definition 5.2 A finite morphism $\phi : Y \to X$ is called *totally ramified* over a closed point P of X if the underlying space of the fibre Y_P consists of a single point Q with $f(Q|P) = 1$. In the case when Y is the spectrum of a discrete valuation ring, we simply say that ϕ is totally ramified if it is totally ramified over the closed point of X.

Totally ramified extensions of discrete valuation rings have the following characterisation, somewhat analogous to Proposition 4.10 (1), (2) but valid for not necessarily henselian rings as well.

Proposition 5.3 *Let $A \subset B$ be an extension of discrete valuation rings with maximal ideals $P \subset Q$, and fraction fields $K \subset L$, respectively. If the induced map $\phi : \operatorname{Spec} B \to \operatorname{Spec} A$ is finite and totally ramified, then $B = A[t]$ with a generator t of Q and the minimal polynomial of t over K is of the form $f = x^e + a_{e-1}x^{e-1} + \ldots + a_0$, where $e = e(Q|P)$, $a_i \in P$ for all i but $a_0 \notin P^2$.*

Conversely, if A is a discrete valuation ring and $B = A[t]$ an extension of the above type, then B is a discrete valuation ring and the map $\operatorname{Spec} B \to \operatorname{Spec} A$ is totally ramified.

A polynomial f as in the statement of the proposition is called an *Eisenstein polynomial.*

Proof: Let v be the discrete valuation associated to B. For the first part, note that the elements $1, t, \ldots, t^{e-1}$ are linearly independent over K. Indeed, assume given a linear combination $a_{e-1}t^{e-1} + \ldots + a_1 t + a_0$ with $a_i \in A$. Since the ramification index is e, for all $a \in A$ the valuation $v(a)$ is divisible by e, and hence the integers $v(a_i t^i)$ are all distinct modulo e. From this we see that $v(\sum a_i t_i) = \min v(a_i t_i)$ and hence the sum cannot be 0. As $[L : K] = e$ by Proposition 1.20 and t is integral over A, we indeed have $L = K(t)$ and $B = A[t] = A[x]/(f)$ with some monic polynomial f. To see that f is of the above type, remark that by the above argument, $f(t) = t^e + a_{e-1}t^{e-1} + \ldots + a_0$ can only be 0 if two of the terms with the smallest valuation have equal valuation. But for $0 < i < e$ the $v(a_i t^i)$ are distinct and nonzero modulo e; on the other hand $v(t^e) = e$. Since $v(a_0)$ is divisible by e the only possibility that remains is $v(a_0) = e$, $v(a_i) \geq e$ for $0 < i < e$.

Conversely, if $B = A[t] = A[x]/(f)$ is of the above type, f is irreducible in $A[x]$ (same proof as over $\mathbf{Z}$), so B is a domain that is finitely generated as an A-module and hence noetherian. The fibre over P is $\operatorname{Spec} \kappa(P)[x]/(x^e)$, from which we see that the last statement holds, but also that B is a local ring whose maximal ideal is generated by t. □

We can now prove the promised formula of Dedekind. To state it we need one more piece of terminology.

Definition 5.4 Let $\phi : Y \to X$ be a finite morphism of Dedekind schemes, and let Q be a branch point of ϕ mapping to a closed point P of X. We say that ϕ is *tamely ramified* at Q if the ramification index $e(Q|P)$ is not divisible by the characteristic of $\kappa(P)$. Otherwise ϕ is *wildly ramified* at Q.

Proposition 5.5 (Dedekind's Different Formula) *Let $\phi : Y \to X$ be a finite morphism of Dedekind schemes such that the corresponding extension $L|K$ of function fields is separable. Let $Q_1, \ldots, Q_n$ be the branch points of ϕ with (not necessarily distinct) images $P_1, \ldots, P_n$ in Y and let $\mathcal{D}_{Y/X} = \mathcal{L}(\sum_i m_i Q_i)$ be the different of ϕ. Then we have*

$$m_i = e(Q_i|P_i) - 1 \text{ if } \phi \text{ is tamely ramified at } Q_i, \text{ and}$$

$$m_i \geq e(Q_i|P_i) \quad \text{if } \phi \text{ is wildly ramified at } Q_i.$$

Proof: Using Proposition 3.9 we may localise and henselise at Q_i and P_i, reducing thereby to the case $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$ with $A \subset B$ henselian discrete valuation rings with maximal ideals $P \subset Q$. Consider the maximal étale subextension $A \subset C \subset B$. Since $\operatorname{Spec} C \to \operatorname{Spec} A$ is étale, we get from the exact sequence in Chapter 6, Lemma 3.5 (2) an isomorphism $\Omega_{B/A} \cong \Omega_{B/C}$. Thus we may assume $A = C$ and so by Proposition 5.3 we have $B = A[t] \cong A[x]/(f)$ with $f \in A[x]$ an Eisenstein polynomial. In this case $\Omega_{B/A}$ is generated by dt and has $f' = 0$ as its single relation, so the different is the ideal generated by $f' = et^{e-1} + (e-1)a_{e-1}t^{e-2} + \ldots + a_1$. If v is the valuation associated to B, here we have $v(a_i) \geq e$ for all i, hence all terms have valuation at least e except for the first in the case $e \notin P$ (i.e. that of tame ramification), when $v(et^{e-1}) = e - 1$. □

It is time for a concrete example.

Example 5.6 Let ℓ be a prime number, ζ a primitive ℓ-th root of unity, $K = \mathbf{Q}(\zeta)$ and $\mathcal{O}_K$ its ring of integers. We analyse the local behaviour of the map $\phi : \operatorname{Spec} \mathcal{O}_K \to \operatorname{Spec} \mathbf{Z}$. For a prime number p (viewed as a closed point of $\operatorname{Spec} \mathbf{Z}$), denote by $\mathbf{Z}_p^h$ the henselisation of $\mathbf{Z}$ at p and $\mathbf{Q}_p^h$ its fraction field. Let B_p be the integral closure of $\mathbf{Z}_p^h$ in $\mathbf{Q}_p^h(\zeta)$.

- For $\ell \neq p$, let C be the maximal étale subextension of $\mathbf{Z}_p^h \subset B_p$ given by Proposition 5.1. Being henselian, it must contain all roots of the equation $x^\ell - 1$ as its residue field does. In particular, it must contain ζ, so it must have the same fraction field as B_p. Since C is also a discrete valuation ring finitely generated as a $\mathbf{Z}_P^h$-module, it must equal B_p, so $\operatorname{Spec} B_p$ is étale over $\operatorname{Spec} \mathbf{Z}_p^h$ and *a fortiori* ϕ is étale at all points of $\mathcal{O}_K$ not lying above ℓ.

- For $\ell = p$, the maximal étale subextension is just $\mathbf{Z}_p^h$ so the map $\operatorname{Spec} B_p \to \operatorname{Spec} \mathbf{Z}_p^h$ is totally ramified. We now show that the degree of the field extension $\mathbf{Q}_p^h(\zeta)|\mathbf{Q}$ is exactly $p-1$, which, together with Proposition 1.20, will imply that the map $\operatorname{Spec} \mathcal{O}_K \to \operatorname{Spec} \mathbf{Z}$ is totally ramified over (ℓ).

  Indeed, the extension $\mathbf{Q}_p^h(\zeta)|\mathbf{Q}$ is of degree at most $p-1$. But it contains the element $1-\zeta$ which is a root of the polynomial F obtained by substituting $1+y$ in place of x in $x^{p-1} + x^{p-2} + \ldots + 1$. One sees immediately that F is an Eisenstein polynomial, so it is irreducible in $\mathbf{Q}_p^h[y]$.

- By Proposition 5.5 we get that the different $\mathcal{D}_{\operatorname{Spec} \mathcal{O}_K/\operatorname{Spec} \mathbf{Z}}$ is the ideal sheaf associated to the divisor $(\ell-2)S$, where S is the unique point lying above (ℓ). We could have obtained this result immediately if we knew that $\mathcal{O}_K = \mathbf{Z}[\zeta]$ but this fact is not obvious; to prove it one commonly uses nearly all the information obtained above.

Remark 5.7 As an amusing application of the previous example we show that any finite abelian group occurs as the Galois group of a finite Galois extension $K|\mathbf{Q}$. Indeed, let A be a finite abelian group of order m and decomposing as a direct sum $A \cong A_1 \oplus \ldots \oplus A_n$ with each A_i cyclic. By Dirichlet's theorem of prime numbers in an arithmetic progression we may find n different prime numbers $\ell_1, \ldots, \ell_n$ each congruent to 1 modulo m. Choose a primitive ℓ_i-th root of unity ζ_i for each i. The Galois group G_i of the Galois extension $\mathbf{Q}(\zeta_i)|\mathbf{Q}$ is cyclic of order $\ell_i - 1$, hence divisible by m and as such has a quotient isomorphic to A_i. Denote by K_i the corresponding Galois extension of $\mathbf{Q}$. For each i the map $\operatorname{Spec} \mathcal{O}_{K_i} \to \operatorname{Spec} \mathbf{Z}$ is étale at the points not mapping to ℓ_i but totally ramified at the unique point lying over ℓ_i; a degree count shows that this implies that we must have $K_i \cap K_j = \mathbf{Q}$ for $i \neq j$. Hence the composite K of the K_i is Galois over $\mathbf{Q}$ with group A.