Contents

Chapter 9
Dedekind domains

The notion of a Dedekind domain allows one to generalize the usual unique factorization in principal ideal domains as in $\mathbb{Z}$ to settings such as the ring of integers in an algebraic number field. In general, a Dedekind domain does not have unique factorization, but the *ideals* in a Dedekind domain do factor uniquely into a product of prime ideals. We shall see that Dedekind domains have a short characterization in terms of the characteristics we have developed.

After this, we shall study the case of an *extension* of Dedekind domains $A \subset B$. It will be of interest to determine how a prime ideal of A factors in B. This should provide background for the study of basic algebraic number theory, e.g. a rough equivalent of the first chapter of [Lan94] or [Ser79].

§1 Discrete valuation rings

1.1 Definition

We start with the simplest case of a *discrete valuation ring,* which is the local version of a Dedekind domain. Among the one-dimensional local noetherian rings, these will be the nicest.

Theorem 1.1 *Let R be a noetherian local domain whose only prime ideals are (0) and the maximal ideal $\mathfrak{m} \neq 0$. Then, the following are equivalent:*

1. *R is factorial.*
2. *$\mathfrak{m}$ is principal.*
3. *R is integrally closed.*
4. *R is a valuation ring with value group $\mathbb{Z}$.*

Definition 1.2 A ring satisfying these conditions is called a **discrete valuation ring** (**DVR**). A discrete valuation ring necessarily has only two prime ideals, namely $\mathfrak{m}$ and (0).

Alternatively, we can say that a noetherian local domain is a DVR if and only if it is of dimension one and integrally closed.

Proof. Assume 1: that is, suppose R is factorial. Then every prime ideal of height one is principal by **??**. But $\mathfrak{m}$ is the only prime that can be height one: it is minimal over any nonzero nonunit of R, so $\mathfrak{m}$ is principal. Thus 1 implies 2, and similarly 2 implies 1 by **??**.

1 implies 3 is true for any R: a factorial ring is always integrally closed, by **??**.

4 implies 2 is easy as well. Indeed, suppose R is a valuation ring with value group $\mathbb{Z}$. Then, one chooses an element $x \in R$ such that the valuation of x is one. It is easy to see that x generates $\mathfrak{m}$: if $y \in \mathfrak{m}$ is a non-unit, then the valuation of y is at least one, so $y/x \in R$ and $y \in (x)$.

The proof that 2 implies 4 is also straightforward. Suppose $\mathfrak{m}$ is principal, generated by t. In this case, we claim that any $x \in R$ is associate (i.e. differs by a unit from) a power of t. Indeed, since $\bigcap \mathfrak{m}^n = 0$ by the Krull intersection theorem (**??**), it follows that there exists n such that x is divisible by t^n but not by t^{n+1}. In particular, if we write $x = ut^n$, then $u \notin (t)$ is a unit. This proves the claim.

With this in mind, we need to show that R is a valuation ring with value group $\mathbb{Z}$. If $x \in R$, we define the valuation of x to be the nonnegative integer n such that $(x) = (t^n)$. One can easily check that this is a valuation on R, which extends to the quotient field by additivity.

The interesting part of the argument is the claim that 3 implies 2. Suppose R is integrally closed, noetherian, and of dimension one; we claim that $\mathfrak{m}$ is principal. Choose $x \in \mathfrak{m} - \{0\}$. If $(x) = \mathfrak{m}$, we are done.

Otherwise, we can look at $\mathfrak{m}/(x) \neq 0$. The module $\mathfrak{m}/(x)$ is finitely generated module a noetherian ring which is nonzero, so it has an associated prime. That associated prime is either zero or $\mathfrak{m}$ because R has dimension one. But 0 is not an associated prime because every element in the module is killed by x. So $\mathfrak{m}$ is an associated prime of $\mathfrak{m}/(x)$.

There is $\overline{y} \in \mathfrak{m}/(x)$ whose annihilator is $\mathfrak{m}$. Thus, there is $y \in \mathfrak{m}$ such that $y \notin (x)$ and $\mathfrak{m}y \subset (x)$. In particular, $y/x \in K(R) - R$, but

$$(y/x)\mathfrak{m} \subset R.$$

There are two cases:

1. Suppose $(y/x)\mathfrak{m} = R$. Then we can write $\mathfrak{m} = R(x/y)$. So $\mathfrak{m}$ is principal. (This argument shows that $x/y \in R$.)

2. The other possibility is that $y/x\mathfrak{m} \subsetneq R$. In this case, $(y/x)\mathfrak{m}$ is an ideal, so

$$(y/x)\mathfrak{m} \subset \mathfrak{m}.$$

   In particular, multiplication by y/x carries $\mathfrak{m}$ to itself, and stabilizes the finitely generated *faithful* module $\mathfrak{m}$. By **??**, we see that y/x is integral over R. In particular, we find that $y/x \in R$, as R was integrally closed, a contradiction as $y \notin (x)$. ▲

Let us give several examples of DVRs.

Example 1.3 The localization $\mathbb{Z}_{(p)}$ at any prime ideal $(p) \neq 0$ is a DVR. The associated valuation is the p-adic valuation.

Example 1.4 Although we shall not prove (or define) this, the local ring of an algebraic curve at a smooth point is a DVR. The associated valuation measures the extent to which a function (or germ thereof) has a zero (or pole) at that point.

Example 1.5 The formal power series ring $\mathbb{C}[[T]]$ is a discrete valuation ring, with maximal ideal (T).

1.2 Another approach

In the proof of Theorem 1.1, we freely used the notion of associated primes, and thus some of the results of **??**. However, we can avoid all that and give a more "elementary approach," as in [CF86].

Let us suppose that R is an integrally closed, local noetherian domain of dimension one. We shall prove that the maximal ideal $\mathfrak{m} \subset R$ is principal. This was the hard part of Theorem 1.1, and the only part where we used associated primes earlier.

Proof. We will show that $\mathfrak{m}$ is principal, by showing it is *invertible* (as will be seen below). We divide the proof into steps:

Step one For a nonzero ideal $I \subset R$, let $I^{-1} := \{x \in K(R) : xI \subset R\}$, where $K(R)$ is the quotient field of R. Then clearly $I^{-1} \supset R$ and I^{-1} is an R-module, but in general we cannot say that $I^{-1} \neq R$ even if I is proper. Nevertheless, we claim that in the present situation, we have

$$\mathfrak{m}^{-1} \neq R.$$

This is the conclusion of Step one.

The proof runs across a familiar line: we show that any maximal element in the set of ideals $I \subset R$ with $I^{-1} \neq R$ is prime. The set of such ideals is nonempty: it contains any (a) for $a \in \mathfrak{m}$ (in which case $(a)^{-1} = Ra^{-1} \neq R$). There must be a maximal element in this set of ideals by noetherianness, which as we will see is prime; thus, that maximal element must be $\mathfrak{m}$, which proves our claim.

So to fill in the missing link, we must prove:

Lemma 1.6 *If S is a noetherian domain, any maximal element in the set of ideals $I \subset S$ with $I^{-1} \neq S$ is prime.*

Proof. Let J be a maximal element, and suppose we have $ab \in J$, with $a, b \notin J$. I claim that if $z \in J^{-1} - S$, then $za, zb \in J^{-1} - S$. The J^{-1} part follows since J^{-1} is a S-module.

By symmetry it is enough to prove the other half for a, namely that $za \notin S$; but then if $za \in S$, we would have $z((a) + J) \subset S$, which implies $((a) + J)^{-1} \neq S$, contradiction, for J was maximal.

Then it follows that $z(ab) = (za)b \in J^{-1} - S$, by applying the claim just made twice. But $ab \in J$, so $z(ab) \in S$, contradiction. ▲

Step two In the previous step, we have established that $\mathfrak{m}^{-1} \neq R$.

We now claim that $\mathfrak{m}\mathfrak{m}^{-1} = R$. First, we know of course that $\mathfrak{m}\mathfrak{m}^{-1} \subset R$ by definition of inverses, and equally $\mathfrak{m} \subset \mathfrak{m}\mathfrak{m}^{-1}$ too. So $\mathfrak{m}\mathfrak{m}^{-1}$ is an ideal sandwiched between $\mathfrak{m}$ and R. Thus we only need to prove that $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$ is impossible. If this were the case, we could choose some $a \in \mathfrak{m}^{-1} - R$ which must satisfy $a\mathfrak{m} \subset \mathfrak{m}$. Then a would integral over R. As R is integrally closed, this is impossible.

Step three Finally, we claim that $\mathfrak{m}$ is principal, which is the final step of the proof. In fact, let us prove a more general claim.

Proposition 1.7 *Let $(R, \mathfrak{m})$ be a local noetherian domain such that $\mathfrak{m}\mathfrak{m}^{-1} = R$. Then $\mathfrak{m}$ is principal.*

Proof. Indeed, since $\mathfrak{m}\mathfrak{m}^{-1} = R$, write

$$1 = \sum m_i n_i, \quad m_i \in \mathfrak{m},\ n_i \in \mathfrak{m}^{-1}.$$

At least one $m_j n_j$ is invertible, since R is local. It follows that there are $x \in \mathfrak{m}$ and $y \in \mathfrak{m}^{-1}$ whose product xy is a unit in R. We may even assume $xy = 1$.

Then we claim $\mathfrak{m} = (x)$. Indeed, we need only prove $\mathfrak{m} \subset (x)$. For this, if $q \in \mathfrak{m}$, then $qy \in R$ by definition of $\mathfrak{m}^{-1}$, so

$$q = x(qy) \in (x).$$ ▲

So we are done in this case too. Taking stock, we have an effective way to say whether a ring is a DVR. These three conditions are much easier to check in practice (noetherianness is usually easy, integral closure is usually automatic, and the last one is not too hard either for reasons that will follow) than the existence of an absolute value.

§2 Dedekind rings

2.1 Definition

We now introduce a closely related notion.

Definition 2.1 A **Dedekind ring** is a noetherian domain R such that

1. R is integrally closed.
2. Every nonzero prime ideal of R is maximal.

Remark If R is Dedekind, then any nonzero element is height one. This is evident since every nonzero prime is maximal.

If R is Dedekind, then R is locally factorial. In fact, the localization of R at a nonzero prime $\mathfrak{p}$ is a DVR.

Proof. $R_{\mathfrak{p}}$ has precisely two prime ideals: (0) and $\mathfrak{p}R_{\mathfrak{p}}$. As a localization of an integrally closed domain, it is integrally closed. So $R_{\mathfrak{p}}$ is a DVR by the above result (hence factorial). ▲

Assume R is Dedekind now. We have an exact sequence

$$0 \to R^* \to K(R)^* \to \mathrm{Cart}(R) \to \mathrm{Pic}(R) \to 0.$$

Here $\mathrm{Cart}(R) \simeq \mathrm{Weil}(R)$. But $\mathrm{Weil}(R)$ is free on the nonzero primes, or equivalently maximal ideals, R being Dedekind. In fact, however, $\mathrm{Cart}(R)$ has a simpler description.

Proposition 2.2 *Suppose R is Dedekind. Then $\mathrm{Cart}(R)$ consists of all nonzero finitely generated submodules of $K(R)$ (i.e. **fractional ideals**).*

This is the same thing as saying as every nonzero finitely generated submodule of $K(R)$ is invertible.

Proof. Suppose $M \subset K(R)$ is nonzero and finitely generated It suffices to check that M is invertible after localizing at every prime, i.e. that $M_{\mathfrak{p}}$ is an invertible—or equivalently, trivial, $R_{\mathfrak{p}}$-module. At the zero prime, there is nothing to check. We might as well assume that $\mathfrak{p}$ is maximal. Then $R_{\mathfrak{p}}$ is a DVR and $M_{\mathfrak{p}}$ is a finitely generated submodule of $K(R_{\mathfrak{p}}) = K(R)$.

Let S be the set of integers n such that there exists $x \in M_{\mathfrak{p}}$ with $v(x) = n$, for v the valuation of $R_{\mathfrak{p}}$. By finite generation of M, S is bounded below. Thus S has a least element k. There is an element of $M_{\mathfrak{p}}$, call it x, with valuation k.

It is easy to check that $M_{\mathfrak{p}}$ is generated by x, and is in fact free with generator x. The reason is simply that x has the smallest valuation of anything in $M_{\mathfrak{p}}$. ▲

What's the upshot of this?

Theorem 2.3 *If R is a Dedekind ring, then any nonzero ideal $I \subset R$ is invertible, and therefore uniquely described as a product of powers of (nonzero) prime ideals, $I = \prod \mathfrak{p}_i^{n_i}$.*

Proof. This is simply because I is in $\mathrm{Cart}(R) = \mathrm{Weil}(R)$ by the above result. ▲

This is Dedekind's generalization of unique factorization.

We now give the standard examples:

Example 2.4 1. Any PID (in particular, any DVR) is Dedekind.

2. If K is a finite extension of $\mathbb{Q}$, and set R to be the integral closure of $\mathbb{Z}$ in K, then R is a Dedekind ring. The ring of integers in any number field is a Dedekind ring.

3. If R is the coordinate ring of an algebraic variety which is smooth and irreducible of dimension one, then R is Dedekind.

4. Let X be a compact Riemann surface, and let $S \subset X$ be a nonempty finite subset. Then the ring of meromorphic functions on X with poles only in S is Dedekind. The maximal ideals in this ring are precisely those corresponding to points of $X - S$.

2.2 A more elementary approach

We would now like to give a more elementary approach to the unique factorization of ideals in Dedekind domains, one which does not use the heavy machinery of Weil and Cartier divisors.

In particular, we can encapsulate what has already been proved as:

Theorem 2.5 *Let A be a Dedekind domain with quotient field K. Then there is a bijection between the discrete valuations of K that assign nonnegative orders to elements of A and the nonzero prime ideals of A.*

Proof. Indeed, every valuation gives a prime ideal of elements of positive order; every prime ideal $\mathfrak{p}$ gives a discrete valuation on $A_{\mathfrak{p}}$, hence on K. ▲

This result, however trivial to prove, is the main reason we can work essentially interchangeably with prime ideals in Dedekind domains and discrete valuations.

Now assume A is Dedekind. A finitely generated A-submodule of the quotient field F is called a **fractional ideal**; by multiplying by some element of A, we can always pull a fractional ideal into A, when it becomes an ordinary ideal. The sum and product of two fractional ideals are fractional ideals.

Theorem 2.6 (Invertibility) *If I is a nonzero fractional ideal and $I^{-1} := \{x \in F : xI \subset A\}$, then I^{-1} is a fractional ideal and $II^{-1} = A$.*

Thus, the nonzero fractional ideals are an *abelian group* under multiplication.

Proof. To see this, note that invertibility is preserved under localization: for a multiplicative set S, we have $S^{-1}(I^{-1}) = (S^{-1}I)^{-1}$, where the second ideal inverse is with respect to $S^{-1}A$; this follows from the fact that I is finitely generated. Note also that invertibility is true for discrete valuation rings: this is because the only ideals are principal, and principal ideals (in any integral domain) are obviously invertible.

So for all primes $\mathfrak{p}$, we have $(II^{-1})_{\mathfrak{p}} = A_{\mathfrak{p}}$, which means the inclusion of A-modules $II^{-1} \to A$ is an isomorphism at each localization. Therefore it is an isomorphism, by general algebra. ▲

The next result says we have unique factorization of **ideals**:

Theorem 2.7 (Factorization) *Each ideal $I \subset A$ can be written uniquely as a product of powers of prime ideals.*

Proof. Let's use the pseudo-inductive argument to obtain existence of a prime factorization. Let I be the maximal ideal which can't be written in such a manner, which exists since A is Noetherian. Then I isn't prime (evidently), so it's contained in some prime $\mathfrak{p}$. But $I = (I\mathfrak{p}^{-1})\mathfrak{p}$, and $I\mathfrak{p}^{-1} \neq I$ can be written as a product of primes, by the inductive assumption. Whence so can I, contradiction.

Uniqueness of factorization follows by localizing at each prime. ▲

Definition 2.8 Let P be the subgroup of nonzero principal ideals in the group I of nonzero ideals. The quotient I/P is called the **ideal class group**.

The ideal class group of the integers, for instance (or any principal ideal domain) is clearly trivial. In general, this is not the case, because Dedekind domains do not generally admit unique factorization.

Proposition 2.9 *Let A be a Dedekind domain. Then A is a UFD if and only if its ideal class group is trivial.*

Proof. If the ideal class group is trivial, then A is a principal ideal domain, hence a UFD by elementary algebra. Conversely, suppose A admits unique factorization. Then, by the following lemma, every prime ideal is principal. Hence every ideal is principal, in view of the unique factorization of ideals. ▲

Lemma 2.10 *Let R be a UFD, and let $\mathfrak{p}$ be a prime ideal which contains no proper prime sub-ideal except for 0. Then $\mathfrak{p}$ is principal.*

The converse holds as well; a domain is a UFD if and only if every prime ideal of height one is principal, by Theorem 1.15.

Proof. First, $\mathfrak{p}$ contains an element $x \neq 0$, which we factor into irreducibles $\pi_1 \dots \pi_k$. One of these, say π_j, belongs to $\mathfrak{p}$, so $\mathfrak{p} \supset (\pi_j)$. Since $\mathfrak{p}$ is minimal among nonzero prime ideals, we have $\mathfrak{p} = (\pi_j)$. (Note that (π_j) is prime by unique factorization.) ▲

Exercise 9.1 This exercise is from [Liu02]. If A is the integral closure of $\mathbb{Z}$ in a number field (so that A is a Dedekind domain), then it is known (cf. [Lan94] for a proof) that the ideal class group of A is *finite*. From this, show that every open subset of $\operatorname{Spec} A$ is a principal open set $D(f)$. Scheme-theoretically, this means that every open subscheme of $\operatorname{Spec} A$ is affine (which is not true for general rings).

2.3 Modules over Dedekind domains

Let us now consider some properties of Dedekind domains.

Proposition 2.11 *Let A be a Dedekind domain, and let M be a finitely generated A module. Then M is projective (or equivalently flat, or locally free) if and only if it is torsion-free.*

Proof. If M is projective, then it is a direct summand of a free module, so it is torsion-free. So we need to show that if M is torsion-free, then it is projective. Recall that to show M is projective, it suffices to show that $M_{\mathfrak{p}}$ is projective for any prime $\mathfrak{p} \subset M$. But note that $A_{\mathfrak{p}}$ is a PID so a module over it is torsion free if and only if it is flat, by Lemma **??**. However, it is also a local Noetherian ring, so a module is flat if and only if it is projective. So $M_{\mathfrak{p}}$ is projective if and only if it is torsion-free, so it now suffices to show that it is torsion-free.

However for any multiplicative set $S \subset A$, if M is torsion-free then M_S is also torsion-free. This is because if

$$\frac{a}{s'} \cdot \frac{m}{s} = 0$$

then there is t such that $tam = 0$, as desired. ▲

Proposition 2.12 *Let A be a Dedekind domain. Then any finitely generated module M over it has (not canonically) a decomposition $M = M^{tors} \oplus M^{tors-free}$.*

Proof. Note that by Lemma **??**, we have a short exact sequence

$$0 \to M^{tors} \to M \to M^{tors-free} \to 0$$

but by proposition 2.11 the torsion free part is projective, so M can be split, not necessarily canonically as $M^{tors} \oplus M^{tors-free}$, as desired. ▲

Note that we may give further information about the torsion free part of the module:

$$M^{tors} = \bigoplus_{\mathfrak{p}} M^{tors}_{\mathfrak{p}}$$

First note that there is a map

$$M^{tors} \to \bigoplus_{\mathfrak{p}} M^{tors}_{\mathfrak{p}}$$

because M is torsion, every element is supported at finitely many points, so the image of f in $M^{tors}_{\mathfrak{p}}$ is only nonzero for finitely many $\mathfrak{p}$. It is an isomorphism, because it is an isomorphism after every localization.

So we have pretty much specified what the torsion part is. We can in fact also classify the torsion free part; in particular, we have

$$M^{tors-free} \simeq \oplus \mathcal{L}$$

where $\mathcal{L}$ are locally free modules of rank 1. This is because we know from above that the torsion free module is projective, we may apply Problem Set 10, Problem 12, and then since L is a line bundle, and I_{-D} is also, $L \otimes I_{-D}$ is a line bundle, and then $M/L \otimes I_{-D}$ is flat, so it is projective, so we may split it off.

Lemma 2.13 *For A a Dedekind Domain, and $I \subset A$ an ideal, then I is a locally free module of rank 1.*

Proof. First note that I is torsion-free and therefore projective by 2.11, and it is also finitely generated, because A is Noetherian. But for a finitely generated module over a Noetherian ring, we know that it is projective if and only if it is locally free, so we have shown that it is locally free.

Also recall that for a module which is locally free, the rank is well defined, i.e, any localization which makes it free makes it free of the same rank. So to test the rank, it suffices to show that if we tensor with the field of fractions K, it is free of rank 1. But note that since K, being a localization of A is flat over A so we have short exact sequence

$$0 \to I \otimes_A K \to A \otimes_A K \to (A/I) \otimes_A K \to 0$$

However, note that $\text{supp}(A/I) = V(\text{Ann}(A/I)) = V(I)$, and the prime (0) is not in $V(I)$, so $A/I \otimes_A K$, which is the localization of A/I at (0) vanishes, so we have

$$I \otimes_A K \simeq A \otimes_A K$$

but this is one-dimensional as a free K module, so the rank is 1, as desired. ▲

We close by listing a collection of useful facts about Dedekind domains. A dozen things every Good Algebraist should R is a Dedekind domain.

1. R is local $\iff$ R is a field or a DVR.
2. R semi-local $\implies$ it is a PID.

3. R is a PID $\iff$ it is a UFD $\iff C(R) = \{1\}$
4. R is the full ring of integers of a number field $K \implies |C(R)| < \infty$, and this number is the *class number* of K.
5. $C(R)$ can be any abelian group. This is Clayborn's Theorem.
6. For any non-zero prime $\mathfrak{p} \in \operatorname{Spec} R$, $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong R/\mathfrak{p}$ as an R-module.
7. "To contain is to divide", i.e. if $A, B \subset R$, then $A \subset B \iff A = BC$ for some $C \subset R$.
8. (Generation of ideals) Every non-zero ideal $B \subset R$ is generated by two elements. Moreover, one of the generators can be taken to be any non-zero element of B.
9. (Factor rings) If $A \subset R$ is non-zero, then R/A is a PIR (**principal ideal ring**).
10. (Steinitz Isomorphism Theorem) If $A, B \subset R$ are non-zero ideals, then $A \oplus B \cong {}_R R \oplus AB$ as R-modules.
11. If M is a finitely generated torsion-free R-module of rank n,[1] then it is of the form $M \cong R^{n-1} \oplus A$, where A is a non-zero ideal, determined up to isomorphism.
12. If M is a finitely generated torsion R-module, then M is uniquely of the form $M \cong R/A_1 \oplus \cdots \oplus R/A_n$ with $A_1 \subsetneq A_2 \subsetneq \cdots \subsetneq A_n \subsetneq R$.

TO BE ADDED: eventually, proofs of these should be added

§3 Extensions

In this section, we will essentially consider the following question: if A is a Dedekind domain, and L a finite extension of the quotient field of A, is the integral closure of A in L a Dedekind domain? The general answer turns out to be yes, but the result is somewhat simpler for the case of a separable extension, with which we begin.

3.1 Integral closure in a finite separable extension

One of the reasons Dedekind domains are so important is

Theorem 3.1 *Let A be a Dedekind domain with quotient field K, L a finite separable extension of K, and B the integral closure of A in L. Then B is Dedekind.*

This can be generalized to the Krull-Akizuki theorem below (**??**).

First let us give an alternate definition of "separable". For a finite field extension k' of k, we may consider the bilinear pairing $k' \otimes_k k' \to k$ given by $x, y \mapsto \operatorname{Tr}_{k'/k}(xy)$. Which is to say $xy \in k'$ can be seen as a k-linear map of finite dimensional vector spaces $k' \to k'$, and we are considering the trace of this map. Then we claim that k' is separable if and only if the bilinear pairing $k' \times k' \to k$ is non-degenerate.

To show the above claim, first note that the pairing is non-degenerate if and only if it is non-degenerate after tensoring with the algebraic closure. This is because if $\operatorname{Tr}(xy) = 0$ for all $y \in k'$, then $\operatorname{Tr}((x \otimes 1_{\overline{k}})y) = 0$ for all $y \in k' \otimes_k \overline{k}$, which we may see to be true by decomposing into pure tensors. The other direction is obtained by selecting a basis of $\overline{k}$ over k, and then noting that for y_i basis elements, if $\operatorname{Tr}(\sum xy_i) = 0$ then $\operatorname{Tr}(xy_i) = 0$ for each i.

[1] The rank is defined as $rk(M) = \dim_{K(R)} M \otimes_R K(R)$ where $K(R)$ is the quotient field.

So now we just need to show that $X = k' \otimes_k \overline{k}$ is reduced if and only if the map $X \otimes_{\overline{k}} X \to \overline{k}$ given by $a \otimes b \mapsto \mathrm{Tr}(ab)$ is non-degenerate. To do this, we show that elements of the kernel of the bilinear map are exactly the nilpotents. But note that X is a finite dimensional algebra over $\overline{k}$, and we may elements as matrices. Then if $\mathrm{Tr}(AB) = 0$ for all B if and only if $\mathrm{Tr}(PAP^{-1}PBP^{-1}) = 0$ for all B, so we may assume A is in Upper Triangular Form. From this, the claim becomes clear.

Proof. We need to check that B is Noetherian, integrally, closed, and of dimension 1.

- Noetherian. Indeed, B is a finitely generated A-module, which obviously implies Noetherianness. To see this, note that the K-linear map $(.,.) : L \times L \to K$, $a, b \to \mathrm{Tr}(ab)$ is nondegenerate since L is separable over K (**??**). Let $F \subset B$ be a free module spanned by a K-basis for L. Then since traces preserve integrality and A is integrally closed, we have $B \subset F^*$, where $F^* := \{x \in K : (x, F) \subset A\}$. Now F^* is A-free on the dual basis of F though, so B is a submodule of a finitely generated A module, hence a finitely generated A-module.
- Integrally closed. B is the integral closure of A in L, so it is integrally closed (integrality being transitive).
- Dimension 1. Indeed, if $A \subset B$ is an integral extension of domains, then $\dim A = \dim B$. This follows essentially from the theorems of "lying over" and "going up." Cf. [Eis95].

So, consequently the ring of algebraic integers (integral over $\mathbb{Z}$) in a number field (finite extension of $\mathbb{Q}$) is Dedekind. ▲

Note that the above proof actually implied (by the argument about traces) the following useful fact:

Proposition 3.2 *Let A be a noetherian integrally closed domain with quotient field K. Let L be a finite separable extension and B the ring of integers. Then B is a finitely generated A-module.*

We shall give another, more explicit proof of Proposition 3.2 whose technique will be useful in the sequel. Let $\alpha \in B$ be a generator of L/K. Let $n = [L : K]$ and $\sigma_1, \ldots, \sigma_n$ the distinct embeddings of L into the algebraic closure of K. Define the **discriminant** of α to be

$$D(\alpha) = \left(\det \begin{bmatrix} 1 & \sigma_1\alpha & (\sigma_1\alpha)^2 & \ldots \\ 1 & \sigma_2\alpha & (\sigma_2\alpha)^2 & \ldots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix} \right)^2 .$$

This maps to the same element under each σ_i, so is in K^* (and even A^* by integrality); it is nonzero by basic facts about vanderMonde determinants since each σ_i maps α to a different element. The next lemma clearly implies that B is contained in a finitely generated A-module, hence is finitely generated (since A is noetherian).

Lemma 3.3 *We have $B \subset D(\alpha)^{-1}A[\alpha]$.*

Proof. Indeed, suppose $x \in B$. We can write $x = c_0(1) + c_1(\alpha) + \ldots c_{n-1}(\alpha^{n-1})$ where each $c_i \in K$. We will show that in fact, each $c_i \in D(\alpha)^{-1}A$, which will prove the lemma. Applying each σ_i, we have for each i, $\sigma_i x = c_0(1) + c_1(\sigma_i\alpha) + \cdots + c_{n-1}(\sigma_i\alpha^{n-1})$. Now by Cramer's lemma, each c_i can be written as a quotient of determinants of matrices involving $\sigma_j x$ and the α^j. The denominator determinant is in fact $D(\alpha)$. The numerator is in K and must be integral, hence is in A. This proves the claim and the lemma. ▲

The above technique may be illustrated with an example.

Example 3.4 Let p^i be a power of a prime p and consider the extension $\mathbb{Q}(\zeta_{p^i})/\mathbb{Q}$ for ζ_{p^i} a primitive p^i-th root of unity. This is a special case of a cyclotomic extension, an important example in the subject. We claim that the ring of integers (that is, the integral closure of $\mathbb{Z}$) in $\mathbb{Q}(\zeta_{p^i})$ is precisely $\mathbb{Z}[\zeta_{p^i}]$. This is true in fact for all cyclotomic extensions, but we will not be able to prove it here.

First of all, ζ_{p^i} satisfies the equation $X^{p^{i-1}(p-1)} + X^{p^{i-1}(p-2)} + \cdots + 1 = 0$. This is because if ζ_p is a p-th root of unity, $(\zeta_p - 1)(1 + \zeta_p + \cdots + \zeta_p^{p-1}) = \zeta_p^p - 1 = 0$. In particular, $X - \zeta_{p^i} \mid X^{p^{i-1}(p-1)} + X^{p^{i-1}(p-2)} + \cdots + 1$, and consequently (taking $X = 1$), we find that $1 - \zeta_{p^i}$ divides p in the ring of integers in $\mathbb{Q}(\zeta_{p^i})/\mathbb{Q}$. This is true for *any* primitive p^i-th root of unity for *any* p^i. Thus the norm to $\mathbb{Q}$ of $1 - \zeta_{p^i}^j$ for any j is a power of p.

I claim that this implies that the discriminant $D(\zeta_{p^i})$ is a power of p, up to sign. But by the vanderMonde formula, this discriminant is a product of terms of the form $\prod(1 - \zeta_{p^i}^j)$ up to roots of unity. The norm to $\mathbb{Q}$ of each factor is thus a power of p, and the discriminant itself plus or minus a power of p.

By the lemma, it follows that the ring of integers is contained in $\mathbb{Z}[p^{-1}, \zeta_{p^i}]$. To get down further to $\mathbb{Z}[\zeta_{p^i}]$ requires a bit more work. **TO BE ADDED:** this proof

3.2 The Krull-Akizuki theorem

We are now going to prove a general theorem that will allow us to remove the separability hypothesis in **??**. Let us say that a noetherian domain has **dimension at most one** if every nonzero prime ideal is maximal; we shall later generalize this notion of "dimension."

Theorem 3.5 (Krull-Akizuki) *Suppose A is a noetherian domain of dimension at most one. Let L be a finite extension of the quotient field $K(A)$, and suppose $B \subset L$ is a domain containing A. Then B is noetherian of dimension at most one.*

From this, it is clear:

Theorem 3.6 *The integral closure of a Dedekind domain in any finite extension of the quotient field is a Dedekind domain.*

Proof. Indeed, by Krull-Akizuki, this integral closure is noetherian and of dimension ≤ 1; it is obviously integrally closed as well, hence a Dedekind domain. ▲

Now let us prove Krull-Akizuki. **TO BE ADDED:** we need to introduce material about length

Proof. We are going to show that for any $a \in A - \{0\}$, the A-module B/aB has finite length. (This is quite nontrivial, since B need not even be finitely *generated* as an A-module.) From this it will be relatively easy to deduce the result.

Indeed, if $I \subset B$ is any nonzero ideal, then I contains a nonzero element of A; to see this, we need only choose an element $b \in I$ and consider an irreducible polynomial

$$a_0 X^n + \cdots + a_n \in K[X]$$

that it satisfies. We can assume that all the $a_i \in A$ by clearing denominators. It then follows that $a_n \in A \cap I$. So choose some $a \in (A \cap I) - \{0\}$. We then know by the previous paragraph (though we have not proved it yet) that B/aB has finite length as an A-module (and a fortiori as a B-module); in particular, the submodule I/aB is finitely generated as a B-module. The exact sequence

$$0 \to aB \to I \to I/aB \to 0$$

shows that I must be finitely generated as a B-module, since the two outer terms are. Thus any ideal of B is finitely generated, so B is noetherian.

TO BE ADDED: B has dimension at most one

To prove the Krull-Akizuki theorem, we are going to prove:

Lemma 3.7 (Finite length lemma) *If A is a noetherian domain of dimension at most one, then for any torsion-free A-module M such that $K(A) \otimes_A M$ is finite-dimensional (alternatively: M has finite rank) and $a \neq 0$, M/aM has finite length.*

Proof. We are going to prove something stronger. If M has rank n and is torsion-free, then will show

$$\ell(M/aM) \leq n\ell(A/aA). \tag{9.1}$$

Note that A/aA has finite length. This follows because there is a filtration of A/aA whose quotients are of the form $A/\mathfrak{p}$ for $\mathfrak{p}$ prime; but these $\mathfrak{p}$ cannot be zero as A/aA is torsion. So these primes are maximal, and A/aA has a filtration whose quotients are *simple*. Thus $\ell(A/aA) < \infty$. In fact, we see thus that *any torsion, finitely-generated module has finite length*; this will be used in the sequel.

There are two cases:

1. M is finitely generated. We can choose generators $m_1, \dots, m_n$ in M of $K(A) \otimes_A M$; we then from these generators get a map
$$A^n \to M$$
which becomes an isomorphism after localizing at $A - \{0\}$. In particular, the kernel and cokernel are torsion modules. The kernel must be trivial (A being a domain), and $A^n \to M$ is thus injective. Thus we have found a finite free submodule $F \subset M$ such that M/F is a torsion module T, which is also finitely generated.

   We have an exact sequence
$$0 \to F/(aM \cap F) \to M/aM \to T/aT \to 0.$$
Here the former has length at most $\ell(F/aF) = n\ell(A/aA)$, and we get the bound $\ell(M/aM) \leq n\ell(A/aA) + \ell(T/aT)$. However, we have the annoying last term to contend with, which makes things somewhat inconvenient. Thus, we use a trick: for each $t > 0$, we consider the exact sequence
$$0 \to F/(a^t M \cap F) \to M/a^t M \to T/a^t T \to 0.$$
This gives
$$\ell(M/a^t M) \leq tn\ell(A/aA) + \ell(T/a^t T) \leq tn\ell(A/aA) + \ell(T).$$
However, $\ell(T) < \infty$ as T is torsion (cf. the first paragraph). If we divide by t, we get the inequality
$$\frac{1}{t}\ell(M/a^t M) \leq n\ell(A/aA) + \frac{\ell(T)}{t}. \tag{9.2}$$
However, the filtration $a^t M \subset a^{t-1} M \subset \cdots \subset aM \subset M$ whose quotients are all isomorphic to M/aM (M being torsion-free) shows that $\ell(M/a^t M) = t\ell(M/aM)$ In particular, letting $t \to \infty$ in (9.2) gives (9.1) in the case where M is finitely generated.

2. M is not finitely generated. Now we can use a rather cheeky argument. M is the inductive limit of its finitely generated submodules $M_F \subset M$, each of which is itself torsion free and of rank at most n. Thus M/aM is the inductive limit of its submodules $M_F/(aM \cap M_F)$ as M_F ranges over We know that $\ell(M_F/(aM \cap M_F)) \leq n\ell(A/aA)$ for each finitely generated $M_F \subset M$ by the first case above (and the fact that $M_F/(aM \cap M_F)$ is a quotient of M_F/aM_F).

But if M/aM is the inductive limit of *submodules* of length at most $n\ell(A/aA)$, then it itself can have length at most $n\ell(A/aA)$. For M/aM must be in fact equal to the submodule $M_F/(aM \cap M_F)$ that has the largest length (no other submodule $M_{F'}/(aM \cap M_{F'})$ can properly contain this). ▲

With this lemma proved, it is now clear that Krull-Akizuki is proved as well.

3.3 Extensions of discrete valuations

As a result, we find:

Theorem 3.8 *Let K be a field, L a finite separable extension. Then a discrete valuation on K can be extended to one on L.*

TO BE ADDED: This should be clarified — what is a discrete valuation?

Proof. Indeed, let $R \subset K$ be the ring of integers of the valuation, that is the subset of elements of nonnegative valuation. Then R is a DVR, hence Dedekind, so the integral closure $S \subset L$ is Dedekind too (though in general it is not a DVR—it may have several non-zero prime ideals) by Theorem 3.1. Now as above, S is a finitely generated R-module, so if $\mathfrak{m} \subset R$ is the maximal ideal, then

$$\mathfrak{m}S \neq S$$

by Nakayama's lemma (cf. for instance [Eis95]). So $\mathfrak{m}S$ is contained in a maximal ideal $\mathfrak{M}$ of S with, therefore, $\mathfrak{M} \cap R = \mathfrak{m}$. (This is indeed the basic argument behind lying over, which I could have just invoked.) Now $S_{\mathfrak{M}} \supset R_{\mathfrak{m}}$ is a DVR as it is the localization of a Dedekind domain at a prime ideal, and one can appeal to **??**. So there is a discrete valuation on $S_{\mathfrak{M}}$. Restricted to R, it will be a power of the given R-valuation, because its value on a uniformizer π is < 1. However, a power of a discrete valuation is a discrete valuation too. So we can adjust the discrete valuation on $S_{\mathfrak{M}}$ if necessary to make it an extension.

This completes the proof. ▲

Note that there is a one-to-one correspondence between extensions of the valuation on K and primes of S lying above $\mathfrak{m}$. Indeed, the above proof indicated a way of getting valuations on L from primes of S. For an extension of the valuation on K to L, let $\mathfrak{M} := \{x \in S : |x| < 1\}$.

§4 Action of the Galois group

Suppose we have an integral domain (we don't even have to assume it Dedekind) A with quotient field K, a finite Galois extension L/K, with B the integral closure in L. Then the Galois group $G = G(L/K)$ acts on B; it preserves B because it preserves equations in $A[X]$. In particular, if $\mathfrak{P} \subset B$ is a prime ideal, so is $\sigma\mathfrak{P}$, and the set $\operatorname{Spec} B$ of prime ideals in B becomes a G-set.

4.1 The orbits of the Galois group

It is of interest to determine the orbits; this question has a very clean answer.

Proposition 4.1 *The orbits of G on the prime ideals of B are in bijection with the primes of A, where a prime ideal $\mathfrak{p} \subset A$ corresponds to the set of primes of B lying over A.*[2] *Alternatively, any two primes $\mathfrak{P}, \mathfrak{Q} \subset B$ lying over A are conjugate by some element of G.*

[2]It is useful to note here that the lying over theorem works for arbitrary integral extensions.

In other words, under the natural map $\operatorname{Spec} B \to \operatorname{Spec} A = \operatorname{Spec} B^G$, the latter space is the quotient under the action of G, while $A = B^G$ is the ring of invariants in B.[3]

Proof. We need only prove the second statement. Let S be the multiplicative set $A - \mathfrak{p}$. Then $S^{-1}B$ is the integral closure of $S^{-1}A$, and in $S^{-1}A = A_{\mathfrak{p}}$, the ideal $\mathfrak{p}$ is maximal. Let $\mathfrak{Q}, \mathfrak{P}$ lie over $\mathfrak{p}$; then $S^{-1}\mathfrak{Q}, S^{-1}\mathfrak{P}$ lie over $S^{-1}\mathfrak{p}$ and are maximal (to be added). If we prove that $S^{-1}\mathfrak{Q}, S^{-1}\mathfrak{P}$ are conjugate under the Galois group, then $\mathfrak{Q}, \mathfrak{P}$ must also be conjugate by the properties of localization. *In particular, we can reduce to the case of* $\mathfrak{p}, \mathfrak{Q}, \mathfrak{P}$ *all maximal.*

The rest of the proof is now an application of the Chinese remainder theorem. Suppose that, for all $\sigma \in G$, we have $\sigma\mathfrak{P} \neq \mathfrak{Q}$. Then the ideals $\sigma\mathfrak{P}, \mathfrak{Q}$ are distinct maximal ideals, so by the remainder theorem, we can find $x \equiv 1 \mod \sigma\mathfrak{P}$ for all $\sigma \in G$ and $x \equiv 0 \mod \mathfrak{Q}$. Now, consider the norm $N_K^L(x)$; the first condition implies that it is congruent to 1 modulo $\mathfrak{p}$. But the second implies that the norm is in $\mathfrak{Q} \cap K = \mathfrak{p}$, contradiction. ▲

4.2 The decomposition and inertia groups

Now, let's zoom in on a given prime $\mathfrak{p} \subset A$. We know that G acts transitively on the set $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ of primes lying above $\mathfrak{p}$; in particular, there are at most $[L : K]$ of them.

Definition 4.2 If $\mathfrak{P}$ is any one of the $\mathfrak{P}_i$, then the stabilizer in G of this prime ideal is called the **decomposition group** $G_{\mathfrak{P}}$.

We have, clearly, $(G : G_{\mathfrak{P}}) = g$.

Now if $\sigma \in G_{\mathfrak{P}}$, then σ acts on the residue field $B/\mathfrak{P}$ while fixing the subfield $A/\mathfrak{p}$. In this way, we get a homomorphism $\sigma \to \overline{\sigma}$ from G into the automorphism group of $B/\mathfrak{P}$ over $A/\mathfrak{p}$ (we don't call it a Galois group because we don't yet know whether the extension is Galois).

The following result will be crucial in constructing the so-called "Frobenius elements" of crucial use in class field theory.

Proposition 4.3 *Suppose $A/\mathfrak{p}$ is perfect. Then $B/\mathfrak{P}$ is Galois over $A/\mathfrak{p}$, and the homomorphism $\sigma \to \overline{\sigma}$ is surjective from $G_{\mathfrak{P}} \to G(B/\mathfrak{P}/A/\mathfrak{p})$.*

Proof. In this case, the extension $B/\mathfrak{P}/A/\mathfrak{p}$ is separable, and we can choose $\overline{x} \in B/\mathfrak{P}$ generating it by the primitive element theorem. We will show that $\overline{x}$ satisfies a polynomial equation $\overline{P}(X) \in A/\mathfrak{p}[X]$ all of whose roots lie in $B/\mathfrak{P}$, which will prove that the residue field extension is Galois. Moreover, we will show that all the nonzero roots of $\overline{P}$ in $B/\mathfrak{P}$ are conjugates of $\overline{x}$ under elements of $G_{\mathfrak{P}}$. This latter will imply surjectivity of the homomorphism $\sigma \to \overline{\sigma}$, because it shows that any conjugate of $\overline{x}$ under $G(B/\mathfrak{P}/A/\mathfrak{p})$ is a conjugate under $G_{\mathfrak{P}}$.

We now construct the aforementioned polynomial. Let $x \in B$ lift $\overline{x}$. Choose $y \in B$ such that $y \equiv x \mod \mathfrak{P}$ but $y \equiv 0 \mod \mathfrak{Q}$ for the other primes $\mathfrak{Q}$ lying over $\mathfrak{p}$. We take $P(X) = \prod_{\sigma \in G}(X - \sigma(y)) \in A[X]$. Then the reduction $\overline{P}$ satisfies $\overline{P}(\overline{x}) = \overline{P}(\overline{y}) = 0$, and $\overline{P}$ factors completely (via $\prod_\sigma (X - \overline{\sigma(t)})$) in $B/\mathfrak{P}[X]$. This implies that the residue field extension is Galois, as already stated. But it is also clear that the polynomial $\overline{P}(X)$ has roots of zero and $\sigma(\overline{y}) = \sigma(\overline{x})$ for $\sigma \in G_{\mathfrak{P}}$. This completes the proof of the other assertion, and hence the proposition. ▲

Definition 4.4 The kernel of the map $\sigma \to \overline{\sigma}$ is called the **inertia group** $T_{\mathfrak{P}}$. Its fixed field is called the **inertia field**.

These groups will resurface significantly in the future.

[3]The reader who does not know about the Spec of a ring can disregard these remarks.

Remark Although we shall never need this in the future, it is of interest to see what happens when the extension L/K is *purely inseparable*.[4] Suppose A is integrally closed in K, and B is the integral closure in L. Let the characteristic be p, and the degree $[L:K] = p^i$. In this case, $x \in B$ if and only if $x^{p^i} \in A$. Indeed, it is clear that the condition mentioned implies integrality. Conversely, if x is integral, then so is x^{p^i}, which belongs to K (by basic facts about purely inseparable extensions). Since A is integrally closed, it follows that $x^{p^i} \in A$.

Let now $\mathfrak{p} \subset A$ be a prime ideal. I claim that there is precisely one prime ideal $\mathfrak{P}$ of B lying above A, and $\mathfrak{P}^{p^i} = \mathfrak{p}$. Namely, this ideal consists of $x \in B$ with $x^{p^i} \in \mathfrak{p}$! The proof is straightforward; if $\mathfrak{P}$ is *any* prime ideal lying over $\mathfrak{p}$, then $x \in \mathfrak{P}$ iff $x^{p^i} \in L \cap \mathfrak{P} = \mathfrak{p}$. In a terminology to be explained later, $\mathfrak{p}$ is *totally ramified*.

[4] Cf. [Lan02], for instance.

CRing Project contents

CRing Project bibliography

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[BBD82] A. A. Beĭlinson, J. Bernstein, and P. Deligne. Faisceaux pervers. In *Analysis and topology on singular spaces, I (Luminy, 1981)*, volume 100 of *Astérisque*, pages 5–171. Soc. Math. France, Paris, 1982.

[Bou98] Nicolas Bourbaki. *Commutative algebra. Chapters 1–7*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[Cam88] Oscar Campoli. A principal ideal domain that is not a euclidean domain. *American Mathematical Monthly*, 95(9):868–871, 1988.

[CF86] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*, London, 1986. Academic Press Inc. [Harcourt Brace Jovanovich Publishers]. Reprint of the 1967 original.

[Cla11] Pete L. Clark. Factorization in euclidean domains. 2011. Available at `http://math.uga.edu/~pete/factorization2010.pdf`.

[dJea10] Aise Johan de Jong et al. *Stacks Project*. Open source project, available at `http://www.math.columbia.edu/algebraic_geometry/stacks-git/`, 2010.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[For91] Otto Forster. *Lectures on Riemann surfaces*, volume 81 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. Translated from the 1977 German original by Bruce Gilligan, Reprint of the 1981 English translation.

[GD] Alexander Grothendieck and Jean Dieudonné. *Élements de géometrie algébrique*. Publications Mathématiques de l'IHÉS.

[Ger] Anton Geraschenko (mathoverflow.net/users/1). Is there an example of a formally smooth morphism which is not smooth? MathOverflow. `http://mathoverflow.net/questions/200` (version: 2009-10-08).

[Gil70] Robert Gilmer. An existence theorem for non-Noetherian rings. *The American Mathematical Monthly*, 77(6):621–623, 1970.

[Gre97] John Greene. Principal ideal domains are almost euclidean. *The American Mathematical Monthly*, 104(2):154–156, 1997.

[Gro57] Alexander Grothendieck. Sur quelques points d'algèbre homologique. *Tôhoku Math. J. (2)*, 9:119–221, 1957.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[Hat02] Allen Hatcher. *Algebraic topology*. Cambridge University Press, Cambridge, 2002. Available at `http://www.math.cornell.edu/~hatcher/AT/AT.pdf`.

[Hov07] Mark Hovey. *Model Categories*. American Mathematical Society, 2007.

[KS06] Masaki Kashiwara and Pierre Schapira. *Categories and sheaves*, volume 332 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2006.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[LR08] T. Y. Lam and Manuel L. Reyes. A prime ideal principle in commutative algebra. *J. Algebra*, 319(7):3006–3027, 2008.

[Mar02] David Marker. *Model theory*, volume 217 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002. An introduction.

[Mat80] Hideyuki Matsumura. *Commutative algebra*, volume 56 of *Mathematics Lecture Note Series*. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., second edition, 1980.

[McC76] John McCabe. A note on Zariski's lemma. *The American Mathematical Monthly*, 83(7):560–561, 1976.

[Mil80] James S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[ML98] Saunders Mac Lane. *Categories for the working mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1998.

[Per04] Hervé Perdry. An elementary proof of Krull's intersection theorem. *The American Mathematical Monthly*, 111(4):356–357, 2004.

[Qui] Daniel Quillen. Homology of commutative rings. Mimeographed notes.

[Ray70] Michel Raynaud. *Anneaux locaux henséliens*. Lecture Notes in Mathematics, Vol. 169. Springer-Verlag, Berlin, 1970.

[RG71] Michel Raynaud and Laurent Gruson. Critères de platitude et de projectivité. Techniques de "platification" d'un module. *Invent. Math.*, 13:1–89, 1971.

[Ser65] Jean-Pierre Serre. *Algèbre locale. Multiplicités*, volume 11 of *Cours au Collège de France, 1957–1958, rédigé par Pierre Gabriel. Seconde édition, 1965. Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1965.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[Ser09] Jean-Pierre Serre. How to use finite fields for problems concerning infinite fields. 2009. arXiv:0903.0517v2.

[SGA72] *Théorie des topos et cohomologie étale des schémas. Tome 1: Théorie des topos*. Lecture Notes in Mathematics, Vol. 269. Springer-Verlag, Berlin, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck, et J. L. Verdier. Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat.

[SGA03] *Revêtements étales et groupe fondamental (SGA 1)*. Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 3. Société Mathématique de France, Paris, 2003. Séminaire de géométrie algébrique du Bois Marie 1960–61. [Algebraic Geometry Seminar of Bois Marie 1960-61], Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin; MR0354651 (50 #7129)].

[Tam94] Günter Tamme. *Introduction to étale cohomology*. Universitext. Springer-Verlag, Berlin, 1994. Translated from the German by Manfred Kolster.

[Vis08] Angelo Vistoli. Notes on Grothendieck topologies, fibered categories, and descent theory. *Published in* FGA Explained, 2008. arXiv:math/0412512v4.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[Wei94] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.