Dedekind rings

Version 3.2 — 27. august 2013 klokken 12:05

If not the main objects of study in algebraic number theory, Dedekind rings are the
ubiquists of the story, and it was in the surroundings of algebraic number theory they
once were born. Attributing the fatherhood to Richard Dedekind is not doing injustice
to anybody.

The class of Dedekind rings studied in algebraic number theory consists mainly of
the rings of algebraic integers in algebraic number fields; although rings of functions
on curves over finite fields are also subjects of study. We shall however not touch upon
them in this course.

These rings are all rather special — also among the Dedekind rings — they are
countable and their all residue fields are finite.

Being Dedekind is a local property of a ring $A$; that is, if $A$ is a noetherian domain,
then $A$ is Dedekind if and only if $A_p$ is Dedekind for all prime ideals $p$. The local
Dedekind rings are just the good old discrete valuation rings. These can be characterized
in many ways; one being that they are local, principal ideal domains, and this property
is the one we chose as a definition. Then, taking the locality of being Dedekind into
account, we shall define a Dedekind ring as a noetherian domain whose localizations
all are DVRs.

Equivalently—as we shall show—a local, noetherian domain is a DVR if and only
if it is of Krull dimension one\(^1\) and integrally closed. As both the property of being
integrally closed and of being of Krull dimension one are local properties (with a slight
liberal interpretation in the latter case), this leads to Dedekind rings being the integrally
closed, noetherian domains of Krull-dimension one.

Discrete Valuation Rings or local Dedekind rings

The discrete valuation rings, which we shall study in this paragraph, are just the local
Dedekind rings, so the paragraph could be presented under the heading “the local study
of Dedekind rings”.

A domain $A$ is said to be a discrete valuation ring — acronymically a DVR — if $A$
is a local, principal ideal domain (acronymically referred to as a PID).

Usually the only maximal ideal in $A$ will be denoted by $m$, and an element $\pi \in A$
generating $m$ is called a uniformizing parameter. Such an element is unique up to
multiplication by a unit in $A$.

The following list summarizes some of properties of a DVR. They all follow easily
from elementary facts about UFDs and PIDs.

\begin{itemize}
  \item $A$ is noetherian. (Every PID is: Consider an ascending chain of ideals $\{a_i\}$, and
        let the ideal $\bigcup \{a_i\}$ be generated by an element $a$, which must be in $a_i$ for some $i$.
        Then $a_j = \bigcup \{a_i\}$ whenever $j \geq i$.)
\end{itemize}

\(^1\)i.e., the maximal ideal is the only prime ideal
A is a UFD. (Every PID is.)

A is integrally closed. (Every UFD is.)

A generator $\pi$ for the maximal ideal $m$ is, up to multiplication with a unit, the only irreducible element in $A$. (If $a$ is irreducible, the principal ideal $(a)$ is maximal, and consequently $(a) = (\pi)$.)

Any element $a \in A$ may in a unique way be represented as a product $a = u\pi^k$ of a unit $u$ and a power $\pi^k$, where $k$ is a non-negative integer. (This holds since $A$ is a UFD whose only irreducible element—up to a unit—is $\pi$.)

The powers $m^k = (\pi^k)$ of the maximal ideal $m$ are the only non-trivial, proper ideals of $A$, and $m$ is the only non-trivial prime ideal in $A$.

We are certainly very interested in the fractional ideals of $A$, and they are as simple as the ideals. They are all principal, generated by powers $\pi^k$—and this time $k$ can be any integer—of any uniformizing parameter $\pi$.

One easily checks the following two statements where $K$ denotes the field of fractions of $A$:

Every element $\alpha \in K$ has a representation $\alpha = u\pi^k$ where $u$ is a unit in $A$ and $k \in \mathbb{Z}$, and this representation is unique (when the parameter $\pi$ is fixed).

Every fractional ideal is principal, i.e., is one of the ideals $m^k = (\pi^k)$ for $k \in \mathbb{Z}$. In particular, they are all invertible. The class group $C_A$ of $A$ is trivial, and the ideal group $I_A$ is canonically isomorphic to $\mathbb{Z}$ with the maximal ideal $m$ as a canonical generator.

**A second characterization** The characterizations of DVRs flourish, but there is one which, at least in our context, is more important, since our main interest is in the rings of algebraic integers. Among the noetherian, local domains of Krull-dimension one, the DVRs are the ones being integrally closed. This paragraph is devoted to a proof of this.

**Proposition 1** Let $A$ be a local, noetherian domain of Krull-dimension one, then $A$ is DVR if and only if $A$ is integrally closed.

**Proof:** We have to show that every ideal in $A$ is principal, and we start by showing that the maximal ideal $m$ is principal. Pick any non-zero element $a \in A$. In the set \{ Ann$(x)$ | $x \in A/(a)A$ \} of ideals there is a maximal element Ann$(z)$ since $A$ is noetherian. Let $b \in A$ be an element whose the residue class mod $(a)A$ is $z$. We claim that:

---

2Of course the parameter $\pi$ can be chosen in many ways which gives different representations, but once it is chosen, the representation is unique.
Ann($z$) = $m$.
Indeed, as Ann($z$) is a non-trivial proper ideal, it suffices to verify that Ann($z$) is prime. So assume that $xyz = 0$. Both $xz \neq 0$ and $yz \neq 0$ does not hold true, since if that were the case, we would have Ann($z$) $\subseteq$ Ann($xz$) as $y \cdot xz = 0$ and $yz \neq 0$; contradicting the maximality of Ann($z$). Hence either $x$ or $y$ lies in Ann($z$).

This translates into

$$b \cdot m \subseteq (a)A \text{ and } (b) \not\subseteq (a).$$

So $b/a \notin A$, but $b/a \cdot m \subseteq A$. We claim that $b/a \cdot m = A$, which shows that $m = (a/b)$. Indeed, $b/a \cdot m$ is an ideal, and if it were a proper ideal, we would have $b/a \cdot m \subseteq m$. The maximal ideal $m$ being finitely generated, this would imply that $b/a$ were integral over $A$, and since $A$ integrally closed, we would have $b/a \in A$. That is not case, so $b/a \cdot m$ is not a proper ideal.

Next, let $a$ be any ideal, we establish that $a$ is not contained in all $(\pi^k)$. If it where, we could invert the descending chain

$$a \subseteq \ldots \subseteq (\pi^i) \subseteq (\pi^{i-1}) \subseteq \ldots \subseteq (\pi)$$

of ideals and obtain the ascending chain of fractional ideals

$$(\pi^{-1}) \subseteq \ldots \subseteq (\pi^{-(i-1)}) \subseteq (\pi^{-i}) \subseteq \ldots \subseteq a^{-1}.$$ They are all submodules of the noetherian module $a^{-1}$, so this chain must be eventually stable. Hence the same applies to the original chain ($\star$) and $(\pi^i) = (\pi^{i+1})$ for some $i$, which is absurd.

To finish off the proof, we let $n = \inf\{ k \in \mathbb{Z} \mid a \not\subseteq (\pi^k) \}$. Then $a \subseteq (\pi^{n-1})$. Pick an element $a \in a$ such that $a \notin (\pi^n)$. We may write $a = u \pi^{n-1}$ for some $u \in A$. Now $u$ can not be in $(\pi)$ since $a$ is not in $(\pi^n)$, and hence $u$ has to be a unit. It follows that $a = (\pi^{n-1})$.

**The ideal group of a DVR** Just to round off this paragraph, we remark that another way of phrasing the fact that any ideal of $A$ is a power of the maximal ideal, is to say that the ideal group $I_A$ of $A$ is canonically isomorphic to $\mathbb{Z}$, a canonical generator being the maximal ideal:

**Proposition 2** Assume that $A$ is a DVR. Then $I_A \simeq \mathbb{Z}$, a generator being the maximal ideal of $A$.

**Valuations** The discrete valuation rings have their name from the concept of a valuation. This is a function, having certain properties, on the set of non-zero elements of the field of fractions $K$ of $A$.

Think of $K$ as some field of functions, like the field of meromorphic functions in some domain $\Omega \subseteq \mathbb{C}$, or the set of rational functions $\mathbb{C}(T)$. At a given point $x$ in $\Omega$ a function has a zero of a certain order or a pole of a certain order, so to any element in $f \in K$, we may associate the integer $\text{ord}_x f$. This is one of the models for a valuation.
Other models, which are closer to algebraic number theory, are the so called \( p \)-adic valuations. In that case, our field \( K \) is the field of rational numbers \( \mathbb{Q} \), and instead of choosing a point \( x \in \Omega \), we choose a prime number \( p \in \mathbb{Z} \). Any rational number \( \alpha \in \mathbb{Q} \) may be written as \( \alpha = u \cdot p^r \) where \( u \) is a rational number, neither whose numerator nor whose denominator has \( p \) as a factor. We put \( v_p(\alpha) = \nu \), and this is the famous \( p \)-adic valuation of \( \alpha \). It enjoys the same formal properties as the order of a function.

The attribute discrete means that the valuation takes values in \( \mathbb{Z} \). A general valuation takes values in an abelian, linearly ordered group, called the value group, and any such group is the value group of some valuation on some field \( K \). However, we shall only meet the discrete ones.

A valuation on the field \( K \) is, in our context, a non-trivial function \( v : K^* \to \mathbb{Z} \) that for all \( x \) and \( y \) from \( K^* \) satisfies the following two conditions:

\[
\begin{align*}
\Box & \quad v(xy) = v(x) + v(y) \\
\Box & \quad v(x + y) \geq \min\{v(x), v(y)\}
\end{align*}
\]

One may give the value \( \infty \) to \( 0 \), and the conditions still hold, and thus regard \( v \) as a function \( v : K \to \mathbb{Z} \cup \{\infty\} \).

The first condition immediately gives \( v(1) = 0 \)—with \( x = y = 1 \) it implies that \( v(1) = v(1) + v(1) \)—and it follows that

\[
\Box \quad v(x^{-1}) = -v(x) \text{ for all } x \neq 0.
\]

The image \( v(K^*) \subseteq \mathbb{Z} \) is a non-trivial subgroup, hence has a positive generator \( e \). In the case that \( e = 1 \)—that is, if \( v \) is surjective— the valuation is said to be normalized. Any valuation can be normalized, just replace \( v \) with \( e^{-1}v \).

Given any valuation \( v \) on a field \( K \), we claim that the set of elements where \( v \) takes non-negative values is a ring, and of course, it is a valuation ring:

**Proposition 3** Assume that \( K \) is a field with a valuation \( v \). Then \( A = \{ x \in K \mid v(x) \geq 0 \} \) is a local \( \text{PID} \), hence a valuation ring. The group of units and the maximal ideal of \( A \) are described by

\[
\begin{align*}
\Box & \quad A^* = \{ x \in K \mid v(x) = 0 \} \\
\Box & \quad m = \{ x \in K \mid v(x) > 0 \}
\end{align*}
\]

**Proof:** The two conditions for \( v \) to be a valuation immediately imply that \( A \) is a subring of \( K \) whose group of units consists of the field elements where \( v \) vanishes. Therefore the set where \( v \) takes positive values, is a unique maximal ideal of \( A \), so \( A \) is local.

If \( a \subseteq A \) is a non-trivial ideal, let \( k \) be the least value \( v \) attains on \( a \), and assume \( k \) is attained at \( a \in a \). Then \( a \) is generated by \( a \). Indeed, if \( b \in a \) is another element, \( v(ba^{-1}) = v(b) - v(a) = v(b) - k \geq 0 \), and consequently \( ba^{-1} \in A \). Hence \( A \) is a \( \text{PID} \). □

---

3 Such groups can be rather complicated, for example will every additive subgroup of the real numbers \( \mathbb{R} \) qualify as one.
Every valuation ring is obtained in the way we just described, and valuations and valuation rings come in pairs. There is just one ambiguity: Two equivalent valuations—that is two valuations $v$ and $w$ on $K$ such that $v(\alpha) = ew(\alpha)$ for some positive integer $e$—obviously define the same valuation ring. But if we restrict our attention to normalized valuations, they correspond in a one to one fashion to DVRs.

Let $K$ be the field of fractions of the valuation ring $A$, and choose a uniformizing parameter $\pi$ in $A$. Any non-zero element if $K$ has a representation $\alpha = u\pi^k$ for some integer $k$, and putting $v(\alpha) = k$, we obtain a valuation on $K$. Of course there is some checking needed, but that is a nice exercise:

**Problem 1.** Show that this gives a well defined function on $K^*$ (i.e., $v$ is independent of the choice of the uniformizing parameter $\pi$) which is a valuation (i.e., $v$ satisfies the two conditions—the first is obvious, the second a little subtler).

---

**Global Dedekind rings**

A noetherian domain $A$ is said to be a **Dedekind ring** or a **Dedekind domain** if for all non-trivial prime ideals $p$ the localization $A_p$ is a DVR. This certainly implies that $A$ is of Krull-dimension one (any chain of prime ideals survive in at least one localization), and since being integrally closed is a local property, the ring $A$ is integrally closed. The converse is easily verified, and the two statements below are equivalent

- $A$ is a Dedekind domain.
- $A$ is an integrally closed, noetherian domain of Krull-dimension one.

**The class group** A very important property of Dedekind rings is that all fractional ideals are invertible — in fact this is another characterization of Dedekind rings, at least among the noetherian domains, but we refrain from proving that. A consequence is that the ideal monoid $I_A$ is a group:

**Proposition 4** Assume that $A$ is a Dedekind ring. Then every non-trivial fractional ideal of $A$ is invertible.

**Proof:** By a local to global argument this follows directly from the inclusion $\mathfrak{a}A^{-1} \subseteq A$ being an identity localized at any prime ideal $p$; indeed, taking products of fractional ideals and forming their inverses commute with localization, and as the local rings $A_p$ all are DVRs, the localized ideals $\mathfrak{a}A_p$ are all invertible.

To any Dedekind ring we may then associate the **ideal group** $I_A$. It has as a subgroup the group $P_A$ consisting of principal ideals. The quotient $C_A = I_A/P_A$ is one of the fundamental invariants of a Dedekind ring. It is called **ideal class group** or, shorter, the **class group** of $A$. When $A$ is the ring of algebraic integers in an algebraic number field $K$, one usually speaks about the **class group of $K$**. In some sense it measures how far ideals in $A$ are from being principal, at least one has

**Proposition 5** If $A$ is Dedekind, then the class group is trivial if and only if $A$ is a PID.
The two groups $I_A$ and $C_A$ sit together with the groups of units $A^*$ and $K^*$ in the exact sequence

$$1 \longrightarrow A^* \longrightarrow K^* \longrightarrow I_A \longrightarrow C_A \longrightarrow 1$$

indeed, one easily convinces one self that $P_A = K^*/A^*$, a generator of a principal ideal in $I_A$ being unique up to a unit.

The class group can be enormously large, in fact any abelian group can occur, but in the realm of rings of algebraic integers, one may — and we shall do it later on — show that the ideal class group is finite. The order is called the class number of the ring (or field), and it is one of the most important and highly mysterious invariants — even for quadratic fields.

Just to mention one example: It still unknown if there are infinitely many real quadratic fields (that is fields $\mathbb{Q}(\sqrt{d})$ with $d$ positive) with class number one. This was conjectured by Gauss. In the imaginary case, however, the nine fields $\mathbb{Q}(\sqrt{-d})$ for $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$ are the only ones whose class number is one. This is a deep theorem with a long and gnarled history — to see that the class numbers of the nine fields equal one, is not to difficult (and I hope we shall have time do that during the course), the hard part is that they are the only ones. For some years one knew that there could at most be one more, and of course the corresponding $d$ had to be astronomically big. The search for the tenth number field with class number one was intense.

**The Fundamental Theorem for Dedekind Rings**

The fundamental theorem of arithmetic states that any integer may be factored as a product

$$n = \pm p_1^{\nu_1} \cdots p_r^{\nu_r}$$

where the $\nu_i$’s are natural numbers which are unambiguously associated to $n$. Letting $\nu_p(n) = \nu_i$ if $p = p_i$ is one of the primes occurring in this factorization, and $\nu_p(n) = 0$ for all other primes, one may express the factorization as

$$n = \pm \prod_{p \text{ prime}} p^{\nu_p(n)}.$$

The fundamental theorem for Dedekind rings is a generalization of this, but involves ideals, not elements from $A$. This is the source of the name ideal: Later on we shall see that many rings of algebraic integers are not UFD s, so the fundamental theorem does not hold true for elements in Dedekind rings. To “save” the situation, Kummer introduce what he called “ideal numbers”, which —as clarified by Dedekind—is nothing but our ideals.

The fundamental theorem states that any ideal $a$ in a Dedekind ring $A$, can be expressed as a product

$$a = p_1^{\nu_1} \cdots p_r^{\nu_r} \quad \text{(※)}$$
where the $\nu_i$’s are natural numbers, which of course are unambiguously associated to the ideal $a$. Just as for the integers, this may also be expressed as “big” product:

$$a = \prod_{p \text{ prime ideal}} p^{\nu_p(a)}$$

where $\nu_p(a) = \nu_i$ for the prime ideals that show up in the product (8), and $\nu_p(a) = 0$ for the rest (by convention $p^0 = A$).

This section is devoted to the proof of this, and in the end, it will be amazingly simple, and based on three observations: The local rings $A_p$ are all DVRs (which allows the definition of the numbers $\nu_p(a)$), any ideal $a$ is contained in just a finite number of prime ideals, and finally, a “local to global” argument gives the equality.

**THE ORDER OF AN IDEAL AT PRIMES** The first task is do define the exponents $\nu_p(a)$ in (8). We will do that for any fractional ideal $a$ right away. Each of the local rings $A_p$ is a DVR, and its fractional ideals are just the powers of the maximal ideal. The localization $aA_p$ is therefore one of these powers, and we let $\nu_p(a)$ be the integer such that

$$aA_p = p^{\nu_p(a)}A_p.$$ 

This defines the number $\nu_p(a)$ canonically. We call $\nu_p(a)$ order of $a$ at $p$ or the multiplicity of $p$ in $a$.

Adopting the terminology from function theory, we sometimes shall say that $a$ has a zero at $p$ if $\nu_p(a) > 0$ and a pole if $\nu_p(a) < 0$, and if our mood tends more toward number theory, we say that $p$ is a factor in $a$, or divides $a$, if $\nu_p(a) > 0$.

Obviously $\nu_p(a) \geq 0$ for any ideal $a$, and the strict inequality $\nu_p(a) > 0$ signifies that $a$ is contained in $p$.

The following two lemmas are useful. The first follows immediately from the fact that localization commutes with the formation of products:

**Lemma 1** Suppose $a$ and $b$ are two fractional ideals in $A$ and let $p$ be a prime ideal. Then

- $\nu_p(ab) = \nu_p(a) + \nu_p(b)$
- $\nu_p(a^{-1}) = -\nu_p(a)$.

**Lemma 2** Assume that $a$ is an ideal and $p$ a prime ideal in $A$. Let $m = pA_p$ be the maximal ideal of $A_p$.

- For any natural number $\nu$ we have $p^{\nu}A_p = m^\nu$. Furthermore it holds that $m^\nu \cap A = p^\nu$.
- For any number $\nu$ it holds that $a \subseteq p^{\nu}$ if and only if $\nu \leq \nu_p(a)$. In particular $a \subseteq p^{\nu_p(a)}$. 

— 7 —
Proof: The first part of the first statement is just that taking products of ideals localizes. For the second part, clearly $p^i \subseteq m^i \cap A$, and if we localize this inclusion at $p$, it becomes an equality after the first part of lemma. If we localize at any other prime $q$, both ideals involved blow up to $A_q$, and the inclusion becomes an equality. Hence, since being iso is a local property of maps, this shows that $m^i \cap A = p^i$.

The second statement follows directly from the first.

Example 1. In $A = \mathbb{Z}[i]$ let us find the different orders of the principal ideal $(2)$.

The ideal $(1+i)$ is prime: Indeed, in $\mathbb{Z}[x]$ the we have the equality $(x^2 + 1, x + 1) = (2, x + 1)$, so $(x^2 + 1, x + 1)$ is prime (the residue field being $\mathbb{F}_2$) since putting $y = x + 1$, we see that $\mathbb{Z}[x]/(2, x + 1) = \mathbb{Z}[y](2, y) = \mathbb{F}_2$.

One computes $(1+i)^2 = (2i) = (2)$ since $i$ is a unit. Hence the order of 2 at $(1+i)$ equals 2. If $p$ is any other prime, $p \cap \mathbb{Z}$ is prime ideal not containing 2, so $(2)A_p = A_p$ and the order is zero.

Example 2. In the ring $\mathbb{Z}[-\sqrt{5}]$ we have equality $(2) = (2, 1 + \sqrt{-5})^2$. Indeed, we compute

$$(2, 1 + \sqrt{-5})^2 = (4, 2(1 + \sqrt{-5}), 2\sqrt{-5} - 4) = (2, 6, 2(1 + \sqrt{-5})) = (2)$$

so the multiplicity of 2 is 2 at $(2, 1 + \sqrt{-5})$ and zero elsewhere. One sees that $(2, 1 + \sqrt{-5})$ is prime because in $\mathbb{Z}[x]$ we have $(x^2 + 5, x + 1, 2) = (2, x + 1)$.

Example 3. We continue with the ring $\mathbb{Z}[-\sqrt{5}]$ and shall decompose the element $\alpha = 1 + \sqrt{-5}$ into a product of primes. The norm of $\alpha$ is $N(\alpha) = \alpha\bar{\alpha} = 6$. Hence both 2 and 3 are the only rational primes in $(\alpha)$. Now $(2) = (2, \alpha)^2$ as we saw. We decompose $(3)$:

$$(x^2 + 5, 3) = (x^2 - 1, 3) = (x - 1, 3) \cap (x + 1, 3),$$

hence $(3)\mathbb{Z}[-\sqrt{5}] = (\sqrt{-5} - 1, 3)(\sqrt{-5} + 1, 3)$ and it follows that

$$\alpha = (\sqrt{-5} + 1, 3)(\sqrt{-5} + 1, 2)$$

(which one by the way easily verifies by computing the product).

Problem 2. Find the order of $(3)$ in the ring $\mathbb{Z}[i]$ at the different primes.

Problem 3. Find the orders of $(26)$ in $\mathbb{Z}[-\sqrt{13}]$ at the different primes.

Ideals are contained in just finitely many primes In this subparagraph we establish this fundamental finiteness property of $A$. It can be done in many ways, and are true for many other rings than the Dedekind rings, but we stick to them. Using that the non-trivial ideals are invertible, makes the proof particularly easy:
Proposition 6 Let \( \{a_n\}_{n \in \mathbb{N}} \) be a descending chain of ideals in the Dedekind ring \( A \) all containing the non-trivial ideal \( a \). Then the chain is stationary, i.e., \( a_{n+1} = a_n \) for \( n >> 0 \).

Proof: Since \( \{a_n\}_{n \in \mathbb{N}} \) is a descending chain of ideals all containing \( a \), the chain \( \{a_n^{-1}\}_{n \in \mathbb{N}} \) is an ascending chain of submodules of the finitely generated module \( a^{-1} \), which must be stationary since \( A \) is noetherian. Since \((a_n)^{-1} = a_n\), the original chain is stationary. \( \Box \)

Proposition 7 If \( a \) is a non-trivial ideal in the Dedekind ring \( A \), then \( a \) is contained in only finitely many prime ideals.

Proof: Assume that \( a \subseteq p_i \) for each \( i \in \mathbb{N} \) where the \( p_i \)'s are non-trivial, proper prime ideals. Let \( a_n = p_1 \cdots p_n \). Then \( \{a_n\}_{n \in \mathbb{N}} \) is a descending chain of ideals all containing \( a \) and by proposition 6 above, it is stationary. Therefore \( p_{n+1}a_n = a_n \) for \( n >> 0 \), which by cancellation gives that \( p_{n+1} = A \). \( \Box \)

Problem 4. This exercise is about the ring \( \mathbb{Z}[\sqrt{-13}] \).

a) Show that \((2, 1 + \sqrt{-13})\) is a prime ideal and that \((2) = (2, 1 + \sqrt{-13})^2\).

b) Show that \((2, 1 + \sqrt{-13})\) is not a principal ideal and that \( \mathbb{Z}[\sqrt{-13}] \) is not UFD.

c) Show that \((7) = (7, 1 + \sqrt{-13})(7, 1 - \sqrt{-13})\) is the factorization in prime ideals.

d) Factor the ideals \((1 + \sqrt{-13})\) and \((\sqrt{-13})\) as a product of prime ideals.

Problem 5. Factor the ideals \((5 + i)\) and \((7 + i)\) in the ring \( \mathbb{Z}[i] \) of Gaussian integers.

Problem 6. Show that the ring \( A = \mathbb{Z}[\sqrt{11}] \) is not integrally closed. Find an ideal \( a \) in \( A \) such that \( aa^{-1} \neq A \).

Problem 7. Let \( d \) be an integer such that \( d \equiv 1 \mod 4 \). Then \( \mathbb{Z}[\sqrt{d}] \) is the ring of integers in \( \mathbb{Q}(\sqrt{d}) \). Let \( p \) be a rational prime.

a) Let \( x \) be an indeterminate. Show that \( \mathbb{Z}[\sqrt{d}] \simeq \mathbb{Z}[x]/(x^2 - d) \) and that

\[
\mathbb{Z}[\sqrt{d}]/(p)\mathbb{Z}[\sqrt{d}] \simeq \mathbb{Z}[x]/(p, x^2 - d) \simeq \mathbb{F}_p[x]/(x^2 - \tilde{d})
\]

where \( \tilde{d} \) denotes the residue class of \( d \mod p \).
b) Show that \((p)\) is a prime ideal in \(\mathbb{Z}[\sqrt{d}]\) if and only if \(x^2 - d\) is irreducible, that is, if and only if \(d\) is not a square mod \(p\). In that case the residue fields equals the field \(\mathbb{F}_{p^2} \cong \mathbb{F}_p(\sqrt{d})\) with \(p^2\) elements.

c) Show that if \(d\) is a square mod \(p\), then \((p) = (p, x - a)(p, x + a)\) where \(a \in \mathbb{Z}\) is such that \(d \equiv a^2 \mod p\).

PROBLEM 8. Show that if \(A\) is a Dedekind ring, then \(A\) is UFD if and only if \(A\) is PID.

PROBLEM 9. Let \(a\) and \(b\) be two elements in the Dedekind ring \(A\). Show that \(\nu_p(a, b) = \min\{\nu_p(a), \nu_p(b)\}\) for all primes \(p\) of \(A\).

PROBLEM 10. Let \(d = 2k\) be an even, squarefree positive integer. Then the ring of integers in \(\mathbb{Q}(\sqrt{-d})\) equals \(\mathbb{Z}[\sqrt{-d}]\).

a) Show that \(p = (2, \sqrt{-d})\) is a prime ideal.

b) Show that \((2) = p^2\).

c) Show that \(p\) is not a principal ideal unless \(d = 2\). HINT: Use that the norm \(N(z) = a^2 + db^2 = \bar{z}z\) is multiplicative.

PROBLEM 11. Let \(d\) be an odd, squarefree positive integer such that \(d \not\equiv -1 \mod 4\). Then the ring of integers in \(\mathbb{Q}(\sqrt{-d})\) equals \(\mathbb{Z}[\sqrt{-d}]\).

a) Show that \(p = (2, 1 + \sqrt{-d})\) is a prime ideal.

b) Show that \((2) = p^2\).

c) Show that \(p\) is not a principal ideal unless \(d = 1\).

PROOF OF THE FUNDAMENTAL THEOREM Finally we bring things together and prove the fundamental theorem, first for ideals, and from there it is easily extended to fractional ideals.

Theorem 1 Let \(A\) be a Dedekind ring and let \(a\) be an ideal. Then

\[
a = \prod_{p \text{ prime}} p^{\nu_p(a)}
\]

PROOF: By the first statement in lemma 2

\[
a \subseteq \bigcap_p p^{\nu_p(a)}.
\]

— 10 —
The different prime ideals $p$ are comaximal (they are in fact maximal ideals) and their intersection thus equals their product. Hence

$$a \subseteq \prod_p p^{\nu_p(a)}.$$  

When localized at the different prime ideals in $A$ this inclusion becomes an identity. Indeed, the product commutes with localization and $aA_p = p^{\nu_p(a)}A_p$ by definition. Hence the theorem follows as being iso is a local property for maps.  

There are two easy but useful consequences:

**Lemma 3** Let $a, b$ be two ideals in the Dedekind ring $A$

- $a \subseteq b$ if and only if $\nu_p(b) \leq \nu_p(a)$ for all prime ideals $p$.
- $a = b$ if and only if $\nu_p(b) = \nu_p(a)$ for all prime ideals $p$.

Concerning the ideal group of $A$ it shows that $I_A$ is the free abelian group generated by the maximal ideals of $A$. That is $I_A \simeq \bigoplus_{p \subseteq A} \mathbb{Z}$, and this isomorphism is canonical.

However, what is subtle, is the image of $P_A$ in $I_A$. In other words, the 10 million dollar question is: Which sequences $(\nu_p)_p$ are order sequences of elements from $A$? This of course, is closely related to computing the ideal class group $C_A$ (which is the quotient group $I_A/P_A$).

A corollary of the fundamental theorem is that a Dedekind ring being a UFD automatically is a PID. Indeed, by the fundamental theorem it suffices to check that the prime ideals are principal. If $p$ is prime, it must contain an irreducible element $\pi$. Since in a UFD being a prime element is equivalent to being irreducible, the principal ideal $(\pi)$ is prime. It follows that $(\pi) = p$ as $A$ is of Krull-dimension one. We have shown:

**Proposition 8** A Dedekind ring $A$ is a UFD is and only if it is a PID.

**An example**

Earlier we mentioned the problem of the tenth quadratic field having class number one. It is fairly easy to see many of the imaginary quadratic fields have class numbers greater than one and to give a flavor of that circle of ideas, let us check that the quadratic fields $\mathbb{Q}(\sqrt{-d})$ where $d > 0$ is squarefree and $d \not\equiv -1 \mod 4$, are among them, except if $d = 1$. For simplicity, we assume that $d$ is odd. Then $d = 2k - 1$ where $k$ is odd. A simplifying fact is that the ring of integers in $\mathbb{Q}(\sqrt{-d})$ equals $\mathbb{Z}[\sqrt{-d}]$ (since $-d \equiv 1 \mod 4$).

The point is that the ideal $(2)$ is ramified in $\mathbb{Z}[\sqrt{-d}]$, as one says, and this is a very small prime to be ramified. In general this means that a prime in the factorization of $(2)$ has a multiplicity exceeding one, but in our modest case it simply means that $(2)$ is a square of a prime ideal. Specifically it is the square:

$$(2) = (2, 1 + \sqrt{-d})^2.$$
This follows by the computation
\[(2, 1 + \sqrt{-d})^2 = (4, 2(1 + \sqrt{-d}), 1 - d + 2\sqrt{-d}) = (4, d + 1, 2(1 + \sqrt{-d})) = (2)\]
since \(d + 1 = 2k\), and \(k\) is odd. Now this implies that \((2, 1 + \sqrt{-d})\) is not a principal ideal, at least if \(d > 1\). Assume it were and let \(x\) be a generator. Then \(2 = u x^2\) for a unit \(u\). Hence
\[4 = N(2) = N(ux^2) = N(u)N(x)^2 = N(x)^2\]
where the norm \(N(z)\) is given as \(N(z) = zz' = a^2 + db^2\) for \(z = a + \sqrt{-db}\). Hence \(N(x) = a^2 + db^2 = 2\), and since \(a\) and \(b\) are integers, this is impossible unless \(d = 1\) and \(a^2 = b^2 = 1\).

**Three consequences of the Chinese remainder theorem**

Given \(r\) points \(x_1, \ldots, x_r\) in \(\mathbb{C}\), and multiplicities \(\nu_1, \ldots, \nu_r\) associated to the points, one easily finds a polynomial having a zero of order exactly \(\nu_i\) at \(x_i\) and no other zeros. Just take the product of the \((x - x_i)^{\nu_i}\) as \(i\) varies from 1 to \(r\). A similar statement, but much weaker, holds true in any Dedekind ring. There are however two important modification.

First, the obvious twist is to replace the \(r\) points by \(r\) prime ideals \(p_1, \ldots, p_r\) and ask for an element \(a\) with \(\nu_{p_i}(a) = \nu_i\). Secondly, and much more substantially, one can no longer guarantee to find elements vanishing only at the specified prime ideals \(p_i\). They might, and often will, have other zeros, away from the given primes.

This result hinges on the Chinese remainder theorem.

**Proposition 9** Assume that \(A\) is a Dedekind ring. Given a sequence \(p_1, \ldots, p_r\) of prime ideals and a sequence of non-negative numbers \(\nu_1, \ldots, \nu_r\). Then there is an element \(a \in A\) such that \(\nu_{p_i}(a) = \nu_i\) for \(i = 1, \ldots, r\).

**Proof:** For each \(i\) chose a non-zero element \(\xi_i\) in \(p_i^{\nu_i}/p_i^{\nu_i+1} \subseteq A/p_i^{\nu_i+1}\) (which can be found since Nakayakama’s lemma guarantees that \(p_i^{\nu_i}/p_i^{\nu_i+1} \neq 0\)). By the Chinese remainder theorem the natural map
\[A \rightarrow \prod_i A/p_i^{\nu_i+1}\]
is surjective, so there is an \(a \in A\) mapping to \((\xi_1, \ldots, \xi_r)\). That is, \(a\) has the property that \(a \in p_i^{\nu_i}A_{p_i}\), but \(a \notin p_i^{\nu_i+1}A_{p_i}\), which after the second part of lemma 2 on page 7 is exactly what we want.

There are two nice applications of this result. The first one is

**Proposition 10** Assume that \(\mathfrak{a}\) is a non-trivial, proper ideal in the Dedekind ring \(A\). Then \(\mathfrak{a}\) is generated by two elements.

**Proof:** Write \(\mathfrak{a} = p_1^{\nu_1} \cdots p_r^{\nu_r}\) for \(i = 1, \ldots, r\). By the proposition there is an element \(a \in \mathfrak{a}\) having the prescribed orders \(\nu_{p_i}(a) = \nu_i\). Unluckily, \(a\) might well have zeros at
other places, and to cope with that, we use another element from $a$, i.e., one that does not vanish at the new zeros introduced by $a$. Therefore we pick the element $b \in A$ such that $\nu_p(b) = \nu_i$ for $i = 1, \ldots, r$, and such that $\nu_p(b) = 0$ whenever $p$ is a prime ideal not among the $p_i$'s such that $\nu_p(a) > 0$. Then $\nu_p(a, b) = \min\{\nu_p(a), \nu_p(b)\} = \nu_p(a)$ for all $p$. Thus $(a, b)$ and $a$ have the same orders everywhere, and consequently, they are equal.

The next one is

**Proposition 11** If a Dedekind ring $A$ has only finitely many prime ideals, then $A$ is a PID.

**Proof:** Let $p_1, \ldots, p_r$ be the finitely many prime ideals of $A$, and let $a = p_1^{\nu_1} \cdots p_r^{\nu_r}$ be an ideal. Pick an element $a \in A$ with $\nu_p(a) = \nu_i$ for $i = 1, \ldots, r$. Then $(a)$ and $a$ have the same orders everywhere, and therefore they are equal. $lacklozenge$