Dedekind Domains

Matthew Warren

Aim: Give small overview of Dedekind domains (DDs)
(note: in a sense DDs are a global version of DVRs, hence is useful to consider them as the integer rings of global/local fields respectively!)

Definition 1 A ring A is a DD if

1. A is a noetherian integral domain
2. A is integrally closed in its field of fractions
3. All nonzero prime ideals of A are maximal.

So, an obvious example of a DD is a PID, my favourite is $\mathbb{Z}$.

One may ask the questions:

- **Q**: Why do we care about DDs?
  A: The rings of integers $\mathcal{O}_K$ of number fields are Dedekind domains (we shall prove this soon enough). Hence if we can prove things about Dedekind domains, and inclusions $A \subset B$ of DDs, then we can prove things about rings of integers!
- **Q**: What nice properties do DDs have?

  A: Many, the most important one is that any ideal of a DD has unique factorisation into prime ideals.

With this in mind, our current aims are:

(a) Prove that $\mathcal{O}_K$ is a DD for K a number field,

(b) Prove that we have unique factorisation into primes.

Lets begin with (a), we prove something more general:

Proposition 1 Suppose that $\mathcal{O}_K$ is a DD with $\mathrm{Frac}(\mathcal{O}_K) = K$, and let L/K be a finite (separable) extension of fields. Then the integral closure $\mathcal{O}_L$ of $\mathcal{O}_K$ in L is also a DD.

So by taking $K = \mathbb{Q}$ and L any number field, we find that $\mathcal{O}_L$ is indeed a DD.

Proving the proposition is basically an exercise in commutative algebra, which we break down into proving the conditions 1,2,3 for a ring to be a DD.

Aim 1: Show that $\mathcal{O}_L$ is integrally closed in L

First, we'll quote some facts that shall be useful

Fact: Let $A \subset B$ be an extensions of rings, then B is a finitely generated A module if and only if B is a finitely generated A-algebra, and B is integral over A.
We say B is finite over A if B is finitely generated as an A-module.

Proof. The proof of this is not difficult, the $\Longleftarrow$ direction is quite easy, the other direction involves being somewhat clever with matrices by taking determinants to give a polynomial. $\square$

This fact is very useful. In particular it implies:

Lemma 1 'Being integral is a transitive property'

ie. if $A \subset B \subset C$ are rings with C integral over B, and B is integral over A, then C is integral over A.

How do we show this? Well, *clearly* being a finite extension of rings is a transitive property. So our idea is to reduce proving that *integrality* is transitive, to showing that *finiteness* is transitive.[1]

Let $x \in C$, then x is integral over B, hence there is a monic $f \in B[X]$ such that $f(x) = 0$. Say $f(X) = X^n + b_{n-1}X^{n-1} + \ldots + b_0$, then we also have $f(X) \in B_0[X]$, where $B_0 := A[b_0, \ldots, b_{n-1}]$.

Notice what we've done here, we've reduced to the case of *finitely generated* rings over A, so that we can use the **Fact** above!
Indeed, invoking the **Fact**, we deduce that B_0 is a finite extension of A, and $B_0[x]$ is a finite extension of B_0. Then because 'finiteness' is transitive we have $B_0[x]$ is finite over A, which in turn implies that x is integral over A.

The discussion above also implies that algebraic closures are in fact rings. We have $x, y \in B$ are both integral over A if and only if $A[x]$ and $A[y]$ are finite A-modules, which holds if and only if $A[x, y]$ is a finite A-module, and thus integral. Hence $x \pm y, xy$ are integral over A.

[1]Compare this to field theory where one shows that being algebraic is transitive, integrality is a refinement of 'algebraic'.

OK! From proposition 2 we deduce that algebraic closures are themselves algebraically closed.

Corollary 1 Let $A \subset B$ be an extension of fields, and $\bar{A}$ the integral closure of A in B. Then $\bar{A}$ is integrally closed in B.

Proof. We have $\bar{A}$ is integral over A by its definition. Suppose $x \in B$ is integral over $\bar{A}$, then by transitivity of integrality we have x integral over A, so $x \in \bar{A}$. $\square$

Therefore we have proven Proposition 1 - $\mathcal{O}_L$ is integrally closed in L ✓.

Aim 2: $\mathcal{O}_L$ is a Noetherian integral domain.

Well, $\mathcal{O}_L$ is clearly an integral domain as is contained in L, and to prove that it is Noetherian we show that it is a finitely generated $\mathcal{O}_K$ module - and use Hilbert's Basis theorem.

Interlude: Trace form and non-degeneracy

Define L/K as above, then the trace form is the symmetric bilinear pairing

$$(,) : L \times L \to K \text{ given by } (x, y) = Tr_{L/K}(xy)$$

This is non-degenerate if and only if L/K is separable. For the $\Longleftarrow$ direction of this statement, we can use the primitive element theorem, the other direction is a bit more involved.

I thought I should quickly note the meaning of non-degeneracy of a bilinear form.
Consider K a field and V a K finite dimensional vector space. A symmetric bilinear form ϕ is non-degenerate if we have $e : V \to \mathrm{Hom}(V, K) =$ such that $e(x) = \phi(x, -)$ is injective.
For symmetric bilinear forms we can think about diagonalizing them, then non-degeneracy holds if and only if this diagonalisation has no zeros.
This becomes of use in the following proposition:

Proposition 2 $\mathcal{O}_K$ is finitely generated over $\mathcal{O}_K$.

Proof. Let e_i be a K-basis of L, by scaling we may assume that e_i are all in $\mathcal{O}_L$. Let $f_i \in L$ be the dual basis with respect to the trace bilinear form, note that this requires non-degeneracy of the trace form! By definition we have $(e_i, f_j) = \delta_{ij}$.

Let $x \in \mathcal{O}_L$, we can write $x = \sum \lambda_i f_i$. Then consider that $e_i x \in \mathcal{O}_L$, hence $(e_i, x) \in \mathcal{O}_K$, and expanding out we find that $(e_i, x) = \lambda_i$.
Hence $\mathcal{O}_L \subset f_1\mathcal{O}_K + \ldots + f_n\mathcal{O}_K = A$. Clearly A is a finitely generated $\mathcal{O}_K$ module - hence a is a Noetherian $\mathcal{O}_K$ module - and $\mathcal{O}_L$ is an $\mathcal{O}_K$ submodule, hence is also Noetherian. $\square$

(Note to self: this is a similar argument to how to prove that the inverse different is a fractional ideal of L) So, the conditions 1,2 of DD's has been proven, all that remains is

Proposition 3 All non-zero prime ideals of $\mathcal{O}_L$ are maximal.

Proof. Let $A \subset B$ be and integral extensions of integral domains, then A is a field if and only if B is a field. A corollary of this is then that if $\mathfrak{p}$ is prime in B and $\mathfrak{q} = A \cap \mathfrak{p}$, then $\frac{A}{\mathfrak{q}} \subset \frac{B}{\mathfrak{p}}$ is an integral extension of integral domains. So $\mathfrak{p}$ is maximal if and only if $\mathfrak{q}$ is maximal. But $\mathfrak{q}$ is a non-zero prime of $\mathcal{O}_K$, which is a DD, so $\mathfrak{q}$ is indeed maximal. Therefore we conclude that $\mathfrak{p}$ is maximal also. $\square$

Cool, so we have proven that $\mathcal{O}_L$ is indeed a Dedekind domain!

Our next result is something that is rather useful for Number fields. We would like to know about the structure of $\mathcal{O}_K$ as an Abelian group. For example, an obvious question is whether $\mathcal{O}_K$ has a $\mathbb{Z}$-basis.

Proposition 4 Let L be a number field of degree n over $\mathbb{Q}$, the integer ring $\mathcal{O}_L$ is a free abelian group of rank n.

Proof. Recall from our proof of Proposition 2 that $\mathcal{O}_L$ is contained in a free Abelian group $A = \bigoplus f_i\mathbb{Z}$ (the sum is direct because f_i are linearly independent over $\mathbb{Q}$). The structure theorem then implies that $\mathcal{O}_L = \bigoplus x_i\mathbb{Z}$ some x_i in $\mathcal{O}_L$ where i ranges from 1 to m, some $m \leq n$. Then note that this equality implies that x_i are a $\mathbb{Q}$-basis for L, hence $m = n$ and we're done. $\square$

Remark: A $\mathbb{Z}$-basis of $\mathcal{O}_L$ is called an integral basis, and is one that minimises the absolute value of $|\Delta(x_i)|$, where $\Delta(x_i) = \det \mathrm{Tr}(x_i x_j)$. Moreover we can generalise the Proposition to L/K where K is a number field with $\mathcal{O}_K$ a PID.

Unique Factorisation in Dedekind Domains

There are multiple paths to this result, one involves looking fractional ideals to show that for ideals $\mathfrak{a}, \mathfrak{b}$ in A (a DD), we have $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{b} \subset \mathfrak{a}$. Here we follow a more theoretical approach.

Two auxiliary lemmas;

Lemma 2 Let R be a Noetherian ring and I a non-zero ideal of R. Then there are non-zero prime ideals $\mathfrak{p}_i$ such that $\mathfrak{p}_1 \dots \mathfrak{p}_r \subset I$

Proof. Suppose this is false, then Noetherian-ness of R implies that there exists a maximal counterexample I to the statement which, in particular, cannot be prime. Then we have $x, y \in R$ such that $xy \in I$, but $x \notin I$ and $y \notin I$. Then the ideals $I + (x)$ and $I + (y)$ contain products of primes by maximality of I, so

$$\big(I + (x)\big)\big(I + (y)\big) = I^2 + (x)I + y(I) + (xy) \subset I$$

contains a product of primes, which is a contradiction. $\square$

Lemma 3 Let R be an integral domain which is integrally closed in $K = \mathrm{Frac}(R)$, and I a non-zero finitely generated ideal of R, and $x \in K$. Then $xI \subset I$ implies $x \in R$

Proof. Consider $I = (f1, ..., fn)$, then we have $xf_i = \sum a_{ij} f_j$, so $(xI - A)\mathbf{f} = 0$ where $\mathbf{f}$ is just the vector (f_i). Multiplying by the adjugate gives $\det(xI - A)\mathbf{f} = 0$, and R an integral domain so $\det(xI - A) = 0$. Therefore x is integral over R, and so is contained in R by integrally closed-ness. $\square$

These two combine to prove:

Theorem 1 *R is a discrete valuation ring (dvr) if and only if R is a DD with exactly one non-zero prime ideal.*

Proof. $\implies$ is clear

For the other direction, R is clearly local so just need to show that its a PID. Let $\mathfrak{m}$ be the unique nonzero prime (hence maximal) ideal. First we show that $\mathfrak{m}$ is principal.

My initial thought was to just choose x in $\mathfrak{m} \setminus \mathfrak{m}^2$ - however would have to prove that this is non-empty first.[2]

Instead consider - $0 \neq x \in m$, we have by Lemma 2 some minimal n such that $\mathfrak{m}^n \subset (x)$ and $\mathfrak{m}^{n-1} \not\subset (x)$. So we may choose $y \in \mathfrak{m}^{n-1} \setminus (x)$, and let $\pi = \frac{x}{y}$. We want to show that $(\pi) = \mathfrak{m}$.
Note that $\pi^{-1} \notin R$ since $y \notin (x)$, and we have $y\mathfrak{m} \subset m^n \subset (x)$, hence $\pi^{-1}\mathfrak{m} \subset R$. If this is not equality, then $\pi^{-1}\mathfrak{m}$ is a proper subset of R hence contained in $\mathfrak{m}$ and so Lemma 3 implies $\pi^{-1} \in R$. Contradiction! Hence $\pi^{-1}\mathfrak{m} = R$ and were done (this also shows that π must be in R).

To complete the proof, we must show that all ideals of R are principal (in fact they must be some power of $\mathfrak{m}$).
Given a proper ideal $I \subset R$, consider the fractional ideals $\pi^{-n}I$. These are strictly increasing, hence (by Noetherian-ness of R) this sequence must eventually *leave* R. Taking the minimal $n + 1$ such that this happens we have $\pi^{-n}I \subset R$, while $\pi^{-n-1}I \not\subset R$. Suppose that $\pi^{-n} \neq R$, then it must be contained within $\mathfrak{m} = \pi$, so $\pi^{-n-1}I \subset R$, which is a contradiction. Therefore $\pi^{-n-1}I$. $\square$

[2] We can actually do this by noting if $\mathfrak{m}$ is not principal, have $x \in \mathfrak{m}$ then lemma 2 says $\mathfrak{m}^n \subset (x) \subsetneq \mathfrak{m}$ so $\mathfrak{m} \neq \mathfrak{m}^n$ some $n > 1$, thus $\mathfrak{m} = \mathfrak{m}^2$.

In particular, consider that

Lemma 4 Given R a Dedekind domain, any non-zero localisation of R is also a DD.

Proof. We can just check the conditions one by one. For example, localisations of Noetherian IDs are Noetherian IDs (though being Noetherian is not a local property and being an ID isn't a local property!), integral closures commute with taking localisations - and the maximal ideals part is clear because the set of primes in $S^{-1}R$ biject with the primes of R that don't intersect S. $\square$

Combining these two results we deduce that

Corollary 2 If R is a DD, then for all $\mathfrak{p}$ nonzero primes in R we have $R_\mathfrak{p}$ DVR.

By definition the DVR $R_\mathfrak{p}$ is the valuation ring of the $\mathfrak{p}$-adic absolute value on Frac$R$. We call the valuation $v_\mathfrak{p}$.
At last, we come to unique factorisation;

Theorem 2 Let R be a Dedekind Domain and $I \subset R$ a proper non-zero ideal. Then I factors into a product of prime ideals.

Proof. Begin by noting the following properties of localisation:

(i) If $I \subsetneq J$ then $IR_\mathfrak{p} \subsetneq JR_\mathfrak{p}$.

(ii) $I = J$ if an only if $IR_\mathfrak{p} = JR_\mathfrak{p}$ for all primes $\mathfrak{p}$

Proving (i) is rather simple, for (ii) the $\implies$ direction is trivial, so consider the converse.
We have $I \subset I + J$, and this is equality if and only if J is contained in I. Now, localisation respects sums (this is clear, since the ideal in the localisation is just the ideal in the localised ring generated by the elements of the ideal.) so we have $I_\mathfrak{p} + J_\mathfrak{p} = I_\mathfrak{p} + I_\mathfrak{p} = I_\mathfrak{p}$. Next, note that taking localisations and taking quotients commute, ie. if A is a ring and M is an A-module with N an A-submodule. Then for any multiplicative S in A we have

$$S^{-1}\left(\frac{M}{N}\right) \cong \frac{S^{-1}M}{S^{-1}N}$$

as $S^{-1}A$ modules. In particular if I, J are ideals in R (hence R modules), we have

$$\left(\frac{I+J}{I}\right)_\mathfrak{p} \cong \frac{I_\mathfrak{p} + J_\mathfrak{p}}{I_\mathfrak{p}}$$

and since we have shown that $I_\mathfrak{p} + J_\mathfrak{p} = I_\mathfrak{p}$, for all prime $\mathfrak{p}$ this implies that $(I + J/I)_\mathfrak{p} = 0$ for all primes. But being zero is a local property, hence we deduce that $I + J/I = 0$, ie $J \subset I$. This argument is completely symmetric in I, J, hence we have $I = J$.

Now we prove the existence of prime factorisation: Let I be an ideal in R, by Lemma 2 above, it contains in some product of primes say

$$I \supset \mathfrak{p}_1^{\beta_1} \dots \mathfrak{p}_n^{\beta_n} = J$$

with all $\beta_i > 0$. Then localising at some prime $\mathfrak{p}$ we have $J_{\mathfrak{p}} = R_{\mathfrak{p}}$ for $\mathfrak{p}$ not in the set of $\mathfrak{p}_i$.

To see this, observe that any two distinct (non-zero) primes are coprime (by maximality) and so $\mathfrak{q}_{\mathfrak{p}} = R_{\mathfrak{p}}$ for $\mathfrak{q} \neq \mathfrak{p}$. Then simply noting that localisation respects products we have the result. Hence we must have $I_{\mathfrak{p}} = R_{\mathfrak{p}}$ for $\mathfrak{p}$ not in the $\mathfrak{p}_i$'s.

Next localise at $\mathfrak{p}_i$, we find let $I_{\mathfrak{p}_i} = \mathfrak{p} R_{\mathfrak{p}}^{\alpha_i}$ for some $\alpha_i \geq 0$. Then by localising at every prime of R, we deduce by (ii) $I = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_n^{\alpha_n}$. $\square$

Uniqueness of such a prime factorisation is simple, in fact one only has to look at the proof for uniqueness in the natural numbers and essentially copy it.