Math 250A, Fall 2004
Homework Assignment #7
Problems due October 26, 2004

Part I: Dedekind Rings.

As we have discussed on the comments page, most authors define a Dedekind ring (or Dedekind domain) to be an integral domain that is Noetherian, of dimension 1 and integrally closed in its fraction field. Being of dimension 1 means that the domain is not a field and that non-zero prime ideals are maximal ideals. In homework #6, you showed that a Dedekind ring à la Lang is Noetherian in Exercise 13 and showed that a Dedekind ring is of dimension 1 in Exercise 18 (at the latest). It is understood in Exercises 13–19 that the ring $\mathfrak{o}$ is not a field; also, Lang has a tendency (or "convention," as he refers to it) to omit mentioning that ideals are non-zero. In the following additional problems, you will show that a Dedekind ring à la Lang is integrally closed in its fraction field.

**1.** *Let $\mathfrak{o}$ be a Dedekind ring, and let $K$ be the fraction field of $\mathfrak{o}$. Suppose that $\mathfrak{a}$ is a fractional ideal of $\mathfrak{o}$. Show that the set $\{\, x \in K \mid x\mathfrak{a} \subseteq \mathfrak{o} \,\}$ coincides with the fractional ideal $\mathfrak{a}^{-1}$.*

Let $I = \{\, x \in K \mid x\mathfrak{a} \subseteq \mathfrak{o} \,\}$. Then $I$ is clearly closed under addition and multiplication by elements of $\mathfrak{o}$. It contains 0, so it's non-empty. Thus it's an $\mathfrak{o}$-submodule of $K$. If $c$ is a non-zero element of $\mathfrak{a}$, then $cI \subseteq \mathfrak{o}$; thus $I$ is a fractional ideal. By definition, $I\mathfrak{a} \subseteq \mathfrak{o}$; on multiplying by $\mathfrak{a}^{-1}$, we find $I \subseteq \mathfrak{a}^{-1}$. Meanwhile, since $\mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathfrak{o}$, $\mathfrak{a}^{-1} \subseteq I$. Conclusion: $I = \mathfrak{a}^{-1}$.

**2.** *Suppose now that $\mathfrak{O}$ (upper-case "$\mathfrak{o}$") is a subring of $K$ that contains $\mathfrak{o}$ and is finite over $\mathfrak{o}$ in the sense that $\mathfrak{O}$ is a finitely generated $\mathfrak{o}$-module. (The action of $\mathfrak{o}$ on $\mathfrak{O}$ is by multiplication inside $\mathfrak{O}$.) Show that $\mathfrak{O}$ is a fractional ideal of $\mathfrak{o}$.*

Each element of $K$ has a denominator: if $x \in K$, then $dx \in \mathfrak{o}$ for some $d \neq 0, d \in \mathfrak{o}$. Since $\mathfrak{O}$ is finitely generated, there is a non-zero $d \in \mathfrak{o}$ such that $d\mathfrak{O} \subseteq \mathfrak{o}$. (Take the product of denominators that work for the generators.) Also, $\mathfrak{O}$ is an $\mathfrak{o}$-submodule of $K$ because it's a ring that contains $\mathfrak{o}$. Hence $\mathfrak{O}$ is a fractional ideal.

*Let $\mathfrak{f}$ be the fractional ideal $\mathfrak{O}^{-1}$, so that*

$$\mathfrak{f} = \{\, x \in K \mid x\mathfrak{O} \subseteq \mathfrak{o} \,\}.$$

*Show that $\mathfrak{f}$ is an integral ideal of $\mathfrak{o}$ and in fact that $\mathfrak{f}$ is even an integral ideal of $\mathfrak{O}$.*

It is clear from the definition that $\mathfrak{f}$ is stable under multiplication by elements of $\mathfrak{O}$. Since it is the inverse of $\mathfrak{O}$ and $\mathfrak{O}$ contains $\mathfrak{o}$, it lies inside $\mathfrak{o}^{-1} = \mathfrak{o}$. Hence it is an ideal of $\mathfrak{o}$ and also an ideal of $\mathfrak{O}$. It is non-zero because it's the inverse of a fractional ideal.

**3.** *Using the inclusion $\mathfrak{f}\mathfrak{O} \subseteq \mathfrak{f}$, show that $\mathfrak{f} = \mathfrak{o}$ and then that $\mathfrak{o} = \mathfrak{O}$. Thus $\mathfrak{o}$ has the maximality property that it is equal to $\mathfrak{O}$ whenever $\mathfrak{O}$ contains $\mathfrak{o}$ and is finite over $\mathfrak{o}$.*

Because $\mathfrak{f} = \mathfrak{O}^{-1}$, $\mathfrak{f}\mathfrak{O} = \mathfrak{o}$. However, $\mathfrak{f}\mathfrak{O} \subseteq \mathfrak{f}$, so we have $\mathfrak{o} \subseteq \mathfrak{f}$, i.e., $\mathfrak{f} = \mathfrak{o}$. Thus $\mathfrak{O}$ is the inverse of $\mathfrak{o}$, so $\mathfrak{O} = \mathfrak{o}$.

**4.** *Suppose that $a \in K$ is integral over $\mathfrak{o}$ in the sense that $a$ satisfies an equation*

$$a^n + c_{n-1}a^{n-1} + \cdots + c_0 = 0$$

*with $c_0, c_1, \ldots, c_{n-1} \in \mathfrak{o}$. Show that $a \in \mathfrak{o}$.*

Let $\mathfrak{O}$ be the smallest subring of $K$ that contains $\mathfrak{o}$ and $a$. This ring is finitely generated over $\mathfrak{o}$. Indeed, it is generated by the set of all $a^i$ $(i = 0, 1, 2, \ldots)$, but $a^n$ can be expressed as an $\mathfrak{o}$-linear combination of lower powers of $a$, $a^{n+1}$ can be expressed in terms of $a, a^2, \ldots, a^n$, and so on. We see that $\mathfrak{O}$ is generated over $\mathfrak{o}$ by $1, a, \ldots, a^{n-1}$, so that in particular it is finitely generated. We see from the problems above that $\mathfrak{O} = \mathfrak{o}$. Thus $a$ lies in $\mathfrak{o}$.

Part II: Fractional ideals in Dedekind rings are projective.

In the following problems, we let $\mathfrak{o}$ be a Dedekind ring.

**5.** *Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are integral ideals that are relatively prime. Show that the natural map $\mathfrak{a} \oplus \mathfrak{b} \to \mathfrak{o}$, $(x + y) \mapsto x + y$ is surjective and that its kernel is $\mathfrak{ab}$. Prove that the $\mathfrak{o}$-modules $\mathfrak{o} \oplus \mathfrak{ab}$ and $\mathfrak{a} \oplus \mathfrak{b}$ are isomorphic.*

The map $\mathfrak{a} \oplus \mathfrak{b} \to \mathfrak{o}$, $(x + y) \mapsto x + y$ is surjective more or less by hypothesis: this is one way of saying that $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime. The kernel of this map is the set of $(x, y) \in \mathfrak{a} \oplus \mathfrak{b}$ such that $x = -y$. This set is the set of all $(t, -t)$ with $t \in \mathfrak{a} \cap \mathfrak{b}$. We have a natural exact sequence

$$0 \to \mathfrak{a} \cap \mathfrak{b} \to \mathfrak{a} \oplus \mathfrak{b} \to \mathfrak{o} \to 0,$$

where the map $\mathfrak{a} \cap \mathfrak{b} \to \mathfrak{a} \oplus \mathfrak{b}$ sends $t$ to $(t, -t)$ and where the next map is the summation map that we are discussing. Because $\mathfrak{o}$ is a free $\mathfrak{o}$-module, the sequence splits, and we get $\mathfrak{a} \oplus \mathfrak{b} \approx \mathfrak{o} \oplus \mathfrak{a} \cap \mathfrak{b}$. This is almost what is required, but we need to see why $\mathfrak{ab}$ and $\mathfrak{a} \cap \mathfrak{b}$ are the same thing.

The ideal $\mathfrak{ab}$ clearly lies both in $\mathfrak{a}$ and $\mathfrak{b}$, so it lies in their intersection. In the other direction, suppose that $t$ is in $\mathfrak{a} \cap \mathfrak{b}$. Because $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime, we can find $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$ so that $x + y = 1$. Then $t = xt + ty$ lies in $\mathfrak{ab}$.

**6.** *Suppose now that $\mathfrak{a}$ and $\mathfrak{b}$ are fractional ideals of $\mathfrak{o}$. (We do not assume that they are integral and we do not assume that they are relatively prime.) Prove that the two $\mathfrak{o}$-modules $\mathfrak{o} \oplus \mathfrak{ab}$ and $\mathfrak{a} \oplus \mathfrak{b}$ are isomorphic.*

The key point is that the isomorphism class of a fractional ideal does not change if we scale the ideal by a non-zero element of $K$: multiplication by $x$ maps $\mathfrak{a}$ to $x\mathfrak{a}$, and an inverse for this map is multiplication by $x^{-1}$. We can thus assume that $\mathfrak{a}$ and $\mathfrak{b}$ are ordinary integral ideals of $\mathfrak{o}$. Moreover, by Problem 19 from last week, we can assume that $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime. In this case, the assertion to be proved is what we just did above.

**7.** *If $\mathfrak{a}$ is a fractional ideal, show that there is an $\mathfrak{o}$-module $M$ so that $\mathfrak{a} \oplus M$ is a free $\mathfrak{o}$-module. Conclude that $\mathfrak{a}$ is a projective $\mathfrak{o}$-module.*

In the above problem, let $\mathfrak{b} = \mathfrak{a}^{-1}$. Then we see that $\mathfrak{a} \oplus \mathfrak{a}^{-1}$ is isomorphic to the free module $\mathfrak{o} \oplus \mathfrak{o}$. Hence $\mathfrak{a}$ is a direct summand of a free module. Accordingly, it is projective.

Part III: one additional problem.

*Do problem 7 on page 353, thus showing that rings that satisfy the standard Dedekind properties have the defining property à la Lang.*

**a.** We have to show that every non-zero ideal of $\mathfrak{o}$ contains a product of primes (= non-zero prime ideals). I understand in this problem that $\mathfrak{o}$ is not a field, i.e., that $\mathfrak{o}$ is smaller than $K$. (If $\mathfrak{o} = K$, one could say that the three hypotheses are actually satisfied: there are no non-zero prime ideals, so the hypothesis about non-zero prime ideals is vacuous.) Then there are non-zero primes because $(0)$ is not a maximal ideal and because there are maximal ideals. So $\mathfrak{o}$ does contain a product of prime ideals: if $\mathfrak{p}$ is a prime, then $\mathfrak{o}$ contains $\mathfrak{p}$, which is a product with one factor. (We could also say that $\mathfrak{o}$ contains $\mathfrak{o}$, which is the product with zero factors.) Also, any prime $\mathfrak{p}$ contains $\mathfrak{p}$, which is again a single-factor product.

Because the ring is Noetherian, it is tempting to use "Noetherian induction" to do this problem. Let $S$ be the set of non-zero ideals of $\mathfrak{o}$ that do *not* contain a product of prime ideals. Assume that $S$ is non-empty. Then $S$ contains a maximal element; let $\mathfrak{a}$ be such an element. Our preliminary remarks show that $\mathfrak{a}$ is a proper ideal of $\mathfrak{o}$ and that it is not a prime ideal. It follows that there are $b, c \in \mathfrak{o}$ so that $bc \in \mathfrak{a}$ but $b$ and $c$ are not in $\mathfrak{a}$. The two ideals $\mathfrak{b} = \mathfrak{a} + (b)$ and $\mathfrak{c} = \mathfrak{a} + (c)$ are then larger than $\mathfrak{a}$ (meaning that they contain $\mathfrak{a}$ but are not equal to $\mathfrak{a}$). One sees easily that their product is $\mathfrak{a}$. By maximality, $\mathfrak{b}$ and $\mathfrak{c}$ each contain products of primes. By multiplying together two inclusions, we see that $\mathfrak{a}$ also contains a product of primes; this contradicts the fact that $\mathfrak{a}$ is in $S$.

**b.** We are to show that every maximal ideal is invertible. I have to confess here that at this point I pulled down off my shelf the van der Waerden book that is alluded to by Lang. This is "Algebra, volume 2" by B. L. van der Waerden, published by Frederick Ungar in 1970. The relevant discussion is in §17.4. Let $\mathfrak{p}$ be a prime of $\mathfrak{o}$ and let $\mathfrak{p}^{-1}$ be defined as in the statement of the problem. (This is the same set as in the first problem of this assignment.) The ideal $\mathfrak{p}\mathfrak{p}^{-1}$ is an integral ideal that contains $\mathfrak{p}$. If it is not $\mathfrak{o}$, then it must be $\mathfrak{p}$, since $\mathfrak{p}$ is maximal. Thus $ab \in \mathfrak{p}$ for each $a \in \mathfrak{p}$ and $b \in \mathfrak{p}^{-1}$. Fix a non-zero element $a$ of $\mathfrak{p}$, and let $b$ be in $\mathfrak{p}^{-1}$. Then $ab \in \mathfrak{p}$, so $ab^2 \in \mathfrak{p}$, and so on; we get that $ab^i \in \mathfrak{p}$ for all $i \geq 0$. It will follow from this that $b$ is integral; thus we have $\mathfrak{p}^{-1} = \mathfrak{o}$.

We first show, however, that the equation $\mathfrak{p}^{-1} = \mathfrak{o}$ is impossible; this will give a contradiction. Take $a \in \mathfrak{p}$, $a \neq 0$. Then $(c)$ contains a product of prime ideals, by part (a). Specifically, suppose that $\mathfrak{p}_1 \cdots \mathfrak{p}_t$ is contained in $(c)$; take $t$ as small as possible in this regard. (In other words, we take the shortest possible product of prime ideals that is contained in $(c)$.) Because $\mathfrak{p}_1 \cdots \mathfrak{p}_t$ is contained in $\mathfrak{p}$, one of the factors, $\mathfrak{p}_1$, say, is contained in $\mathfrak{p}$. Because primes are maximal, $\mathfrak{p}_1$ and $\mathfrak{p}$ are equal. Now the product $\mathfrak{p}_2 \cdots \mathfrak{p}_t$ cannot be contained in $(c)$ because $t$ was supposed to be minimal. This means that there is some $x$ in $\mathfrak{p}_2 \cdots \mathfrak{p}_t$ that is not in $(c)$. Because the full product $\mathfrak{p}_1 \cdots \mathfrak{p}_t$ is in $(c)$, $x\mathfrak{p} \subseteq (c) = c\mathfrak{o}$, so that $x/c \in \mathfrak{p}^{-1}$. Note finally that $x/c$ is not in $\mathfrak{o}$ because $x$ is not in $(c)$. Accordingly, $\mathfrak{p}^{-1}$ is bigger than $\mathfrak{o}$.

We now want to show that $b \in \mathfrak{o}$ if there is a non-zero $a \in \mathfrak{o}$ such that $ab^i \in \mathfrak{o}$ for all $i$. Consider the subring $R = \mathfrak{o}[b]$ of $K$. This ring consists of all $\mathfrak{o}$-linear combinations of the powers $b^i$ of $b$. The product $aR$ is an $\mathfrak{o}$-submodule of $\mathfrak{o}$, i.e., an ideal of $\mathfrak{o}$. Because $\mathfrak{o}$ is Noetherian, $aR$ is finitely generated over $\mathfrak{o}$. Since multiplication by the non-zero element $a$ is an isomorphism of $\mathfrak{o}$-modules $R \xrightarrow{\sim} aR$, $R$ is finitely generated over $\mathfrak{o}$. This means that $b$ is integral over $\mathfrak{o}$; indeed, the finite generation of $R$ over $\mathfrak{o}$ is condition **INT 2** on page 334 of Lang. Because $\mathfrak{o}$ is assumed to be integrally closed in $K$, $b$ lies in $\mathfrak{o}$.

**c.** To show that every non-zero ideal of $\mathfrak{o}$ is invertible, it now suffices to show that every such ideal is a product of primes of $\mathfrak{o}$. This is what we do. More precisely, we prove by induction on $n$: if $\mathfrak{a}$ contains a product of $n$ prime ideals, then $\mathfrak{a}$ is invertible. By part (a), every $\mathfrak{a}$ contains some product of primes, so the inductive assertion covers what we need to do. The case $n = 0$ corresponds to the case where $\mathfrak{a} = \mathfrak{o}$; here, I'd say that $\mathfrak{o}$ is the empty product of ideals. (If you don't like that, just say that $\mathfrak{o}$ is clearly invertible and stick to proper ideals $\mathfrak{a}$.) If $n = 1$, then $\mathfrak{a}$ contains a single prime $\mathfrak{p}$. Then $\mathfrak{a} = \mathfrak{p}$ because primes are maximal, and we are OK by part (b).

Let's suppose that $n$ is bigger than 1 and that $\mathfrak{a}$ contains $\mathfrak{p}_1 \cdots \mathfrak{p}_n$. Once again, if $\mathfrak{a} = \mathfrak{o}$, there is nothing to show, so we can and do assume that $\mathfrak{a}$ is proper. Then $\mathfrak{a}$ is contained in some maximal ideal $\mathfrak{m}$. Because $\mathfrak{m}$ contains the product $\mathfrak{p}_1 \cdots \mathfrak{p}_n$, it contains one of the factors $\mathfrak{p}_i$. As above, we can and will assume that $i = 1$. We have

$$\mathfrak{m}\mathfrak{p}_2 \cdots \mathfrak{p}_n \subseteq \mathfrak{a} \subseteq \mathfrak{m}.$$

Multiply by $\mathfrak{m}^{-1}$ to get

$$\mathfrak{m}\mathfrak{p}_2 \cdots \mathfrak{p}_n \subseteq \mathfrak{a}\mathfrak{m}^{-1} \subseteq \mathfrak{o}.$$

The ideal $\mathfrak{b} := \mathfrak{a}\mathfrak{m}^{-1}$ is thus an integral ideal that contains a product of $n - 1$ primes. It is invertible by induction. Then $\mathfrak{m}^{-1}\mathfrak{b}^{-1}$ is an inverse for $\mathfrak{a} = \mathfrak{m}\mathfrak{b}$.