Math 250A, Fall 2001
Homework Assignment #6
Problems due October 19, 2004

Problems from Lang's book: Chapter II, Problems 13–19

Let's start by trying to figure out what we're talking about. It seems to me that the ring $\mathfrak{o} = K$ is actually an example of a Dedekind ring in Lang's definition. However, the usual definition of a Dedekind ring (also called a Dedekind domain) requires that the ring be of dimension 1; this means that (0) is a prime ideal but not a maximal ideal and that all non-zero prime ideals are maximal ideals. So I will assume $\mathfrak{o} \neq K$. The fractional ideals are subgroups of K of the form xI, where x is a non-zero element of K and I is a non-zero ideal of $\mathfrak{o}$. The product of two ideals I and J of $\mathfrak{o}$ is the smallest ideal of $\mathfrak{o}$ that contains all products ab with $a \in I$, $b \in J$. It consists of (finite) sums $\sum a_k b_k$ with $a_k \in I$ and $b_k \in J$.

13. Let $\mathfrak{a}$ be a non-zero ideal of $\mathfrak{o}$ and let $\mathfrak{b}$ be the inverse of $\mathfrak{a}$ in the group of fractional ideals of $\mathfrak{o}$. Then $\mathfrak{a}\mathfrak{b} = \mathfrak{o}$; note that $\mathfrak{o}$ is the identity element of the group. Hence $1 \in \mathfrak{a}\mathfrak{b}$, so that $1 = \sum a_i b_i$, where $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$. For each $a \in \mathfrak{a}$, we have $a = \sum (ab_i)a_i$. Since $ab_i \in \mathfrak{o}$, it follows that a belongs to the ideal generated by the a_i.

14. Since we now know that every ideal of $\mathfrak{o}$, is finitely generated, $\mathfrak{o}$ is a Noetherian ring. As we discussed in class on October 14, $\mathfrak{o}$ satisfies the so-called ascending chain condition. This means that if we have ideals $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$ with $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \ldots$, the chain stabilizes after some point: there's an N such that $\mathfrak{a}_n = \mathfrak{a}_N$ for all $n \geq N$. As we discussed in class, we may infer that every non-empty set of ideals of $\mathfrak{o}$ has a maximal element (cf. the proof of Theorem 5.2 on page 112).

We prove first that all non-zero ideals of $\mathfrak{o}$ are products of prime ideals. Needless to say, prime ideals can be so written (as a product with one factor). Also, it's a convention that the ring $\mathfrak{o}$ itself can be so written—as the empty product! Consider the set S of ideals of $\mathfrak{o}$ that cannot be written as a product of prime ideals. We want to see that the set is empty. (I am attempting to follow the argument in class that shows that elements in a PID are product of irreducible elements provided that they are non-zero and are not units.) Assume that S is non-empty and let $\mathfrak{a}$ be a maximal element of S. Thus $\mathfrak{a}$ cannot be written as a product of primes but that all ideals that strictly contain $\mathfrak{a}$ may be written as products of primes. Note that $\mathfrak{a}$ is a proper ideal because $\mathfrak{o}$ is the empty product of primes. By Zorn's lemma, we may choose a maximal ideal $\mathfrak{m}$ of $\mathfrak{o}$ that contains $\mathfrak{a}$. We have $\mathfrak{a} = \mathfrak{m}(\mathfrak{m}^{-1}\mathfrak{a})$. Since $\mathfrak{m}^{-1}\mathfrak{a} \subseteq \mathfrak{m}^{-1}\mathfrak{m} = \mathfrak{o}$, $\mathfrak{m}^{-1}\mathfrak{a}$ is an ideal of $\mathfrak{o}$. Because $\mathfrak{m}$ is smaller than $\mathfrak{o}$, $\mathfrak{m}^{-1}\mathfrak{a}$ contains $\mathfrak{a}$ but isn't equal to $\mathfrak{a}$. By the maximality of $\mathfrak{a}$ as a counterexample, $\mathfrak{m}^{-1}\mathfrak{a}$ is a product of primes, say $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$. Then $\mathfrak{a} = \mathfrak{m}\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$ is also a product of prime ideals.

Next, we show that non-zero prime ideals of $\mathfrak{o}$ are maximal. (Note: this is Exercise 18, so we can skip #18 later on.) Suppose $\mathfrak{p}$ is a non-zero prime and that we have $\mathfrak{p} \subseteq \mathfrak{a}$ with $\mathfrak{a}$ an ideal of $\mathfrak{o}$. Then $\mathfrak{p} = \mathfrak{a}(\mathfrak{a}^{-1}\mathfrak{p})$, where the two factors $\mathfrak{a}$ and $\mathfrak{a}^{-1}\mathfrak{p}$ are ideals of $\mathfrak{o}$. An important, but easy, fact about commutative rings is that if a prime ideal contains a product $\mathfrak{a}\mathfrak{b}$ of two ideals, then it contains at least one of the ideals. Indeed, suppose that $\mathfrak{p}$ contains $\mathfrak{a}\mathfrak{b}$ and does not contain $\mathfrak{a}$. Then there is an $a \in \mathfrak{a}$ with $a \notin \mathfrak{p}$. Since $ab \in \mathfrak{p}$ for each $b \in \mathfrak{b}$ and since $\mathfrak{p}$ is prime, $\mathfrak{p}$ contains all $b \in \mathfrak{b}$ and therefore contains $\mathfrak{b}$. Now our $\mathfrak{p}$ is equal to the product $\mathfrak{a}(\mathfrak{a}^{-1}\mathfrak{p})$, so it must contain either $\mathfrak{a}$ or $\mathfrak{a}^{-1}\mathfrak{p}$. The first alternative gives $\mathfrak{a} = \mathfrak{p}$ and the second gives $\mathfrak{a} = \mathfrak{o}$. Thus $\mathfrak{p}$ is maximal.

To finish, we must prove the uniqueness of expressions of a non-zero ideal as a product of primes. Suppose that $\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$, where the factors are all primes. The first factor $\mathfrak{p}_1$ divides (i.e., contains) the product $\mathfrak{q}_1 \cdots \mathfrak{q}_s$, so it must divide one of the factors, say q_1. We have then $\mathfrak{p}_1 \supseteq \mathfrak{q}_1$; the maximality of $\mathfrak{q}_1$ gives the equality of $\mathfrak{p}_1$ and $\mathfrak{q}_1$. The uniqueness that we need follows by the standard inductive argument.

15. Consider the prime factorization of (t). There's only one prime, so $(t) = \mathfrak{p}^n$ for some n. Since $(t) \subseteq \mathfrak{p}$ but (t) is not contained in $\mathfrak{p}^2$, we must have $n = 1$.

A question that is suggested by this problem is whether or not there is a t in $\mathfrak{p}$ but not in $\mathfrak{p}^2$. If not, $\mathfrak{p} = \mathfrak{p}^2$. By Problem 13, $\mathfrak{p}$ is generated by a finite number of elements, say $a_1, \ldots, a_r$. We take r as small as possible here. Note that r is positive because $\mathfrak{p}$ is a non-zero prime ideal of $\mathfrak{o}$. We then have $\mathfrak{p} = \mathfrak{o}a_1 + \cdots + \mathfrak{o}a_r$, so that $\mathfrak{p} = \mathfrak{p}^2 = \mathfrak{p}a_1 + \cdots \mathfrak{p}a_r$. Since $a_r \in \mathfrak{p}$, a_r may be written as a sum $b_1a_1 + \cdots b_ra_r$ for some $b_1, \ldots, b_r$ in $\mathfrak{p}$. Hence $a_r(1-b_r) = \displaystyle\sum_{i=1}^{r-1} a_ib_i$. Now $1-b_r$ is not in $\mathfrak{p}$ because b_r is in $\mathfrak{p}$ while 1 is not in $\mathfrak{p}$. Since $\mathfrak{p}$ is the unique maximal ideal of $\mathfrak{o}$, $1-b_r$ must be a unit of $\mathfrak{o}$. (The ideal $(1-b_r)$ is contained in no maximal ideal and thus must be the unit ideal.) Hence a_r can be expressed as an $\mathfrak{o}$-linear combination of $a_1, \ldots, a_{r-1}$ and is therefore a redundant generator of $\mathfrak{p}$. In other words, $\mathfrak{p}$ can be generated by the $r-1$ elements $a_1, \ldots, a_{r-1}$; this is contrary to the minimality of r. (See the discussion of Nakayama's Lemma, p. 424, for the origin of this argument.)

Added later: a simpler argument would have been to say that the equation $\mathfrak{p} = \mathfrak{p}^2$ contradicts the unique factorization of ideals into primes! So the Nakayama argument is not necessary.

16. If $\mathfrak{p} = 0$, then $\mathfrak{o}_\mathfrak{p} = K$, which I would prefer not to regard as a Dedekind ring. So let's take $\mathfrak{p} \neq 0$. The ring $\mathfrak{o}_\mathfrak{p}$ is a subring of K that is smaller than K. It has (0) as a prime ideal, but (0) is not maximal. As we proved above, once we see that $\mathfrak{o}_\mathfrak{p}$ is a Dedekind ring, we will know that all its non-zero primes are maximal. On the other hand, Exercise 3 shows that $\mathfrak{o}_\mathfrak{p}$ has exactly one maximal ideal. Hence $\mathfrak{o}_\mathfrak{p}$ has exactly one non-zero prime ideal if it's a Dedekind ring.

To show that $\mathfrak{o}_\mathfrak{p}$ is a Dedekind ring, it will be helpful to consult the bottom 2/5 of page 110, where we consider localizations A_S. Here's a general fact that could have been mentioned in this set-up. Namely, the map ψ_S sets up a 1-1 correspondence between ideals of A that are disjoint from S and the proper ideals of $S^{-1}A$. When S is the complement of a prime ideal $\mathfrak{p}$, an ideal of A is disjoint from S exactly when it's contained in $\mathfrak{p}$. When you localize A at $\mathfrak{p}$ (i.e., when you take $S = A \setminus \mathfrak{p}$, you get a ring $A_\mathfrak{p}$ all of whose proper ideals are contained in $S^{-1}\mathfrak{p}$. The ideal $S^{-1}\mathfrak{p}$ is then the unique maximal ideal of $A_\mathfrak{p}$; this ring is local.

Now we take $A = \mathfrak{o}$ and take S to be the complement in A of a non-zero prime ideal $\mathfrak{p}$. We need to check that ψ_S sets up a map from fractional ideals of A to fractional ideals of $S^{-1}A$. This map is compatible with multiplication. It's also surjective because a fractional ideal of $S^{-1}A$ is the product of a usual (integral) ideal of $S^{-1}A$ and an element of the field of fractions of A and because ψ_S is surjective on integral ideals. It follows that $S^{-1}A$ is a Dedekind domain: we can find an inverse for each fraction ideal of $S^{-1}A$. In sum, it's a Dedekind ring with a unique maximal ideal.

By the previous exercise (and my discussion showing that there is always a t as in the exercise), we see that the unique maximal ideal of $\mathfrak{o}_\mathfrak{p}$ is principal. It is generated by t whenever t lies in the localization of $\mathfrak{p}$ but not in the square of the localization. Pick t, but note that t has the form x/y, where $y \in \mathfrak{o}$ is not in $\mathfrak{p}$ and x is in $\mathfrak{o}$. Some reflection should convince you that x lies in $\mathfrak{p}$ but not in $\mathfrak{p}^2$. In other words, when we express (x) as a product of prime ideals, $\mathfrak{p}$ occurs exactly once in the expression. For each $n \geq 0$, the ideal $(x^n) = (x)^n$ has $\mathfrak{p}^n$, but not $\mathfrak{p}^{n+1}$, in its prime factorization. We will use this remark in doing out Problem 19.

17. We are dealing with regular old non-zero ideals of $\mathfrak{o}$. If $\mathfrak{a}|\mathfrak{b}$, then $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, where $\mathfrak{c}$ is an integral ideal of $\mathfrak{o}$. Then $\mathfrak{b} = \mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}$. Conversely, if $\mathfrak{b} \subseteq \mathfrak{a}$, then $\mathfrak{b} = (\mathfrak{a}\mathfrak{a}^{-1})\mathfrak{b}$ may be written $\mathfrak{a}\mathfrak{c}$, where $\mathfrak{c}$ is the integral ideal $\mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{o}$.

For part (b), we note that $\mathfrak{a} \subseteq \mathfrak{a}+\mathfrak{b}$ and $\mathfrak{b} \subseteq \mathfrak{a}+\mathfrak{b}$, so that $\mathfrak{a}+\mathfrak{b}$ divides both $\mathfrak{a}$ and $\mathfrak{b}$ (in the sense of this exercise). Conversely, if $\mathfrak{c}$ divides both $\mathfrak{a}$ and $\mathfrak{b}$, then it contains each of these ideals, so it contains (i.e., divides) their sum.

19. If $\mathfrak{a}$ is a non-zero ideal of $\mathfrak{o}$ and $\mathfrak{p}$ is a prime of $\mathfrak{o}$ (i.e., a non-zero prime ideal of $\mathfrak{o}$), let $\operatorname{ord}_\mathfrak{p} \mathfrak{a}$ be the exponent of $\mathfrak{p}$ in the unique factorization of $\mathfrak{a}$ as a product of prime ideals. If x is a non-zero element of $\mathfrak{o}$, write $\operatorname{ord}_\mathfrak{p} x$ for $\operatorname{ord}_\mathfrak{p}(x)$. It is easy to see that the two versions of "ord" extend uniquely to homomorphisms from the group of fractional ideals of $\mathfrak{o}$ and the group K^* to the group of integers under addition. As we saw in the solution to Problem 16, for each $e \geq 0$ and each $\mathfrak{p}$, we can find an $x \in \mathfrak{o}$ such that $\operatorname{ord}_\mathfrak{p} x = e$. Next, if $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ are distinct primes, and if $(e_1, \ldots, e_t)$ is a t-tuple of non-negative integers, then we can find $x \in \mathfrak{o}$ such that $\operatorname{ord}_{\mathfrak{p}_i} x = e_i$ for each $i = 1, \ldots, t$. This follows from the previous remark and the Chinese Remainder Theorem: for each i, we take x_i such that $\operatorname{ord}_{\mathfrak{p}_i} x_i = e_i$, and then we take a single $x \in \mathfrak{o}$ such that $x \equiv x_i \bmod \mathfrak{p}_i^{e_i+1}$ for all i.

In the context of the problem, first find a $y \in \mathfrak{o}$ so that $\operatorname{ord}_\mathfrak{p} y = \operatorname{ord}_\mathfrak{p} \mathfrak{a}$ for all $\mathfrak{p}$ dividing $\mathfrak{a}$. We then find an x such that

$$\operatorname{ord}_\mathfrak{p} x = \begin{cases} 0 & \text{for all } \mathfrak{p}|\mathfrak{a} \\ \operatorname{ord}_p y & \text{for all } \mathfrak{p}|(y), \mathfrak{p} \not|\mathfrak{a} \\ 0 & \text{for all } \mathfrak{p}|\mathfrak{b}, \mathfrak{p} \not|(y). \end{cases}$$

If I've done this right, the fractional ideal $\dfrac{x}{y}\mathfrak{a}$ is actually an integral ideal that is prime to $\mathfrak{b}$ (and also to $\mathfrak{a}$).