MATH 503: HOMEWORK #1

DUE FRIDAY, FEB. 1, 5 P.M. YING ZONG'S MAILBOX

1. Discrete valuation rings

1.1. Show that every discrete valuation $v : \mathbb{Q}^* \to \mathbb{Z}$ has the form $v = v_p$ for some prime p, where as in class, $v_p(r) = \mathrm{ord}_p(r)$ for all non-zero $r \in \mathbb{Z}$.

Hints: In class we showed $v(1) = 0$. Show that $v(r) \geq 0$ if $0 \neq r \in \mathbb{Z}$. Prove that $\{0\} \cup \{r \in \mathbb{Z} : v(r) > 0\}$ is a non-zero prime ideal of $\mathbb{Z}$.

1.2 Suppose A is a subring of a ring B. One says that B is integral over A if each element $b \in B$ satisfies an equation of the form

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

where $n \geq 1$ and $a_0, \ldots, a_{n-1}$ are in A. Suppose now that B is integral over A, A and B are integral domains, and that $v : K^* \to \mathbb{Z}$ is a discrete valuation of the fraction field K of B. Show that if $v(a) \geq 0$ for all $a \in A$ then $v(b) \geq 0$ for $b \in B$.

1.3 With the notation of problem 1.2, suppose $A = \mathbb{Z}$ and that B is the ring $\mathbb{Z}[i]$ of Gaussian integers. Show B is integral over A. Suppose $v : \mathbb{Q}(i)^* \to \mathbb{Z}$ is a discrete valuation of $\mathbb{Z}[i]$. Prove that $v(a) \geq 0$ for $0 \neq a \in A$ and deduce that $v(b) \geq 0$ for $0 \neq b \in B$. Then show all discrete valuations of B have the form $v_{\mathcal{P}} = \mathrm{ord}_{\mathcal{P}}$ where $\mathcal{P}$ is a prime ideal of B and $\mathrm{ord}_{\mathcal{P}}(\alpha) = m$ when $0 \neq \alpha \in B$ and $m \geq 0$ is the largest non-negative integer such that $\alpha \in \mathcal{P}^m$.

Comments: Use the ideas in problem 1.1 together with the fact that B is a P. I. D.. In fact, the conclusion of this problem is true much more generally. An algebraic number field K is a field containing $\mathbb{Q}$ which is a finite dimensional vector space over $\mathbb{Q}$. The ring of integers O_K of K is the set of all $\alpha \in K$ which are integral over $\mathbb{Z}$. We will hopefully have time to show later that O_K is in fact a ring and that there are a finite number of elements of O_K such that every other element is an integral linear combination of these elements. Given that O_K is a ring, you might try to show that the discrete valuations of O_K are exactly the $v_{\mathcal{P}} = \mathrm{ord}_{\mathcal{P}}$ associated to the prime ideals $\mathcal{P}$ of O_K. This is more difficult to show if O_K is not a P.I.D., and in fact the question of determining whether O_K is a P.I.D. is a central problem in algebraic number theory. There are only a finite number of K known for which O_K is a P. I. D..

2. Euclidean rings and P.I.D.'s

2.1 The sequence of Fibonacci numbers are defined by $F_0 = 1$, $F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for $n \geq 1$. Suppose that in the Euclidean algorithm for finding the g.c.d of two integers a and b, we always choose q and r so $a = qb + r$ and $0 \leq r < b$. How many applications of the division algorithm are needed to find the g.c.d of F_{n+1} and F_n? What is this g.c.d.?

2.2. Show that if R is a P. I. D. and D is a multiplicatively closed subset of R, then $D^{-1}R$ is a P. I. D.

3. U.F.D.'s

3.1 Do problem 5 of §8.3 of Dummit and Foote.