Solutions to Homework 8

Math 600, Fall 2007

36 (10 points) Dummit-Foote, 8.2 #6
Let R be a domain in which every prime ideal is principal. This exercise proves that R is a PID.

a) Assume that the set of non-principal ideals of R is nonempty. If $\{I_\alpha\}$ is a totally ordered set of such ideals then, $\cup_\alpha I_\alpha$ cannot be principal (otherwise some I_α would be principal) and hence is an upper bound for $\{I_\alpha\}$. By Zorn's lemma, the non-principal ideals have a maximal element. Denote one such maximal element by I.

b) and c): Let I be as in part a). Since I is not prime, we have $a, b \in R$ with $ab \in I$ but $a, b \notin I$. By the maximal property of I we have $I_a = I + (a)$ is principal, let $I_a = (\alpha)$. Let $J = \{r \in R \,|\, rI_a \subset I\}$. Since J contains I and b, it is strictly larger than I and hence principal, let $J = (\beta)$. Since $I \subset (\alpha)$, it follows that $I = (\alpha) \cdot J = (\alpha\beta)$ contradicting the non-principality of I, thus the set of non-principal ideals of R is empty, or R is a PID.

37 (10 points) Dummit-Foote, 8.2 #8

Every ideal in $S^{-1}R$ is of the form $S^{-1}I$ where I is an ideal in R (prove). The principality of I then implies that of $S^{-1}I$.

38 (10 points) Dummit-Foote, 8.3 #5

a) The usual norm on $\mathbb{C}$ when restricted to R gives a norm $N(a + b\sqrt{-n}) = a^2 + nb^2$. When $n > 3$, the norms of 2, $\sqrt{-n}$, and $1 \pm \sqrt{-n}$ cannot be written as a product of norms, hence these elements are irreducible.

b) Suppose $\sqrt{-n}$ is prime. This in turn forces n to be a prime, indeed: let $n = n_1 \cdot n_2$ with n_1 and n_2 being relatively prime square-free integers. Then, the primality of $\sqrt{-n}$ together with the fact that $\sqrt{-n} \,|\, n$ implies, $\sqrt{-n} \,|\, n_1$ and considering norms we get $n \,|\, n_1^2$ which is impossible, therefore n is a prime and odd since $n > 3$. Further, consider the factorization $n = 2 \cdot (1 + n)/2$. Clearly $1 + \sqrt{-n}$ does not divide 2 by considering norm. We can show that $1 + \sqrt{-n}$ does not divide $(1 + n)/2$ either, indeed: let $(1 + \sqrt{-n})(a + b\sqrt{-n}) = (1 + n)/2$ and taking norm, we see that there are no solutions for a, b. This shows that $(1+\sqrt{-n})$ is not a prime. Therefore we have showed that one of $1+\sqrt{-n}$ or $\sqrt{-n}$ is not prime. However, in a UFD every irreducible is prime (prove), therefore R cannot be a UFD. The ring of integers in $\mathbb{Q}(\sqrt{-n})$ is $\mathbb{Z}(\sqrt{-n})$ when $-n \equiv 2, 3 \pmod 4$. Thus for such $n > 3$ (square-free) the ring of integers is not a UFD.

c) From part b), one of $(1+\sqrt{-n})$ or $(\sqrt{-n})$ is a non-prime which we denote by a. If $\mathfrak{m}$ is a maximal ideal containing (a) then, $\mathfrak{m}$ cannot be principal. To see this suppose $\mathfrak{m}$ is principal, then either $\mathfrak{m} = (a)$ (impossible since maximal ideals are prime, but (a) is not prime) or a is reducible (impossible since both choices of a are irreducible). Thus $\mathfrak{m}$ is a nonprincipal ideal.

39 (10 points) Dummit-Foote, 9.2 #4

There are infinitely many primes in any UFD, by Euclid's proof. Suppose $\{p_1, p_2, \cdots p_n\}$ is a list of the primes in the UFD. Let p be a prime occuring in the unique factorization of the element $p_1 \cdot p_2 \cdots p_n + 1$. Then $p \neq p_i$ because $p_i \not| p_1 \cdot p_2 \cdots p_n + 1$.

40 (10 points) Let R be a domain, $a \in R - \{0\}$, and let I be the ideal in $R[X]$ generated by a and X. Show that I is principal only if $a \in R^\times$.

The ideal (a, x) is the set of polynomials with constant term divisible by a. Therefore we observe that $a \in R^\times \Leftrightarrow (a, x) = R[x]$. Suppose (a, x) is principal with $(a, x) = (p(x))$. Because R is a domain, $p(x)$ must have degree 0 for a to be in $(p(x))$. So $p(x) = p_0$. Now for x to be in $(p(x)) = (p_0)$, we must have that $p_0 \in R^\times$. But this implies $(a, x) = (p_0) = R[x]$, which by the observation made in the beginning implies $a \in R^\times$.

41 (10 points) Let $\omega \in \mathbb{C}$ be a solution of $X^3 = 1$ with $\omega \neq 1$. Let $R = \{a + b\omega \,|\, a, b \in \mathbb{Z}\}$. Clearly R is a domain. Show R is a PID.

Let N be the usual norm on $\mathbb{C}$ restricted to R. (Note that $N(x + y\omega) = x^2 + y^2 - xy$). It suffices to show that R is a Euclidean domain with respect to N. Given $\alpha = a + b\omega$ and $\beta = c + d\omega$, let $q = \alpha/\beta \in \mathbb{C}$. Clearly q is in the subfield $\{x + y\omega \,|\, x, y \in \mathbb{Q}\}$ which we denote by $\mathbb{Q}(\omega)$. Write $q = x + y\omega$ and set $q_1 = \lfloor x \rfloor + \lfloor y \rfloor \omega$ and $q_2 = q - q_1$ where $\lfloor x \rfloor$ is the greatest integer less than or equal x. We have $\alpha = q_1\beta + r$ where all quantities are in R and $r = (q - q_1) \cdot \beta$. Clearly, $N(q - q_1) \leq 0.25 + 0.25 + 0.25 = 0.75$ and thus $N(r) < N(\beta)$, showing that R is a Euclidean domain.