MATH 603, SPRING 2011
HOMEWORK ASSIGNMENT #9 ON DEDEKIND DOMAINS AND COMPLETIONS: SOLUTIONS

JONATHAN ROSENBERG

(1) Let $R = \mathbb{R}[x,y]/(x^2+y^2-1)$.

(a) To show R is a Dedekind domain, we can apply the theorem proved in class, that it suffices to show R is the integral closure of the PID $S = \mathbb{R}[x]$ in a finite extension field of $K = \mathbb{R}(x)$ (the field of fractions of $\mathbb{R}[x]$). Let $L = \mathbb{R}(x)[y]/(y^2+x^2-1)$. This is a finite algebraic extension of K of degree 2, since $1-x^2$ is not a perfect square in K. Any element of L can be represented by an expression $f(x,y) = k_1(x) + k_2(x)y$ with $k_1(x)$, $k_2(x) \in K$. If $f(x,y)$ (here we mean the image in L) is integral over S, then so is its Galois conjugate $k_1(x) - k_2(x)y$, so adding and subtracting, we see $k_1(x)$ and $k_2(x)y$ are integral over S. But S is integrally closed in K, so $k_1(x) \in S$, and since y is integral over S, being a root of the monic polynomial $y^2 - (1-x^2)$, $k_2(x)y^2 = k_2(x)(1-x^2)$ is also integral over S. That means $k_2(x)(1-x^2)$ lies in K and is integral over S, and so is a polynomial in x. So $k_2(x) = g(x)/(1-x^2)$ with $g(x) \in S$. Since $k_2(x)y$ is integral over S, so is

$$(k_2(x)y)^2 = \frac{g(x)^2(1-x^2)}{(1-x^2)^2} = \frac{g(x)^2}{1-x^2},$$

which can only happen if $g(x)$ is divisible by $1-x^2$. So then $k_1(x)$ and $k_2(x)$ are in S and $f(x,y) \in R$.

(b) Let P be a non-zero prime ideal of R; then its contraction $P \cap S$ to $S = \mathbb{R}[x]$ is a prime idea of S. If $P \cap S = (0)$, then $(0) \subset R$ and P would be nested prime ideals both lying over $(0) \subset S$, which is impossible by A-M Corollary 5.9 Thus $P \cap S$ is a non-zero prime ideal and R/P is a finite extension field of $S/(P \cap S)$. But every maximal ideal of $\mathbb{R}[x]$ is of codimension 1 or 2, and the quotient by this maximal ideal is either $\mathbb{R}$ or $\mathbb{C}$ (the only finite extensions of $\mathbb{R}$), so R/P is a finite extension field of $\mathbb{R}$ and is isomorphic to $\mathbb{R}$ or $\mathbb{C}$. In the other direction, by the Lying Over Theorem, R must have at least one prime ideal lying over every maximal ideal of $\mathbb{R}[x]$. Now we distinguish various cases.

(i) The maximal ideals of $S = \mathbb{R}[x]$ of codimension 1 are all of the form $(x-\alpha)$, $\alpha \in \mathbb{R}$. Suppose $|\alpha| \leq 1$. Then there exists $\beta \in \mathbb{R}$, $|\beta| \leq 1$, unique up to sign, with $\alpha^2 + \beta^2 = 1$. The ideal $P = (x-\alpha, y-\beta)$ of R has codimension 1, so is maximal with $R/P \cong \mathbb{R}$, and $P \cap S = (x-\alpha)$. We claim that all prime ideals P lying over $(x-\alpha)$ when $\alpha \in \mathbb{R}$, $|\alpha| \leq 1$, are of this form. If we extend scalars from $\mathbb{R}$ to $\mathbb{C}$, i.e., we look at $R \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}[x,y]/(x^2+y^2-1)$, then since every maximal ideal of $\mathbb{C}[x,y]$ is the kernel of evaluation at some point of $\mathbb{C}^2$, P must be the contraction to R of the kernel of evaluation at (α,β), where $\beta \in \mathbb{C}$ and $\alpha^2 + \beta^2 = 1$. But since $1 - \alpha^2 \geq 0$ in our case, any such β is real and satisfies $|\beta| \leq 1$, $\alpha^2 + \beta^2 = 1$, as required.

(ii) Suppose P is a maximal ideal of R lying over $(x-\alpha)$ in $S=\mathbb{R}[x]$, but this time with $|\alpha|>1$. Then P must be the contraction to R of $(x-\alpha, y-\beta)$, where $\beta\in\mathbb{C}$ and $\alpha^2+\beta^2=1$. Since $\beta^2=1-\alpha^2<0$, $\beta=i\gamma$ is purely imaginary, with $\gamma\in\mathbb{R}$, $\gamma^2=\alpha^2-1\geq 0$. Then P contains $(y-\beta)(y-\overline{\beta})=y^2+\gamma^2=y^2+\alpha^2-1$ as well as $x-\alpha$. But $y^2+\alpha^2-1$ is congruent mod x^2+y^2-1 to $-(x^2-\alpha^2)$, which already lies in $(x-\alpha)$, and in fact, in this case, $(x-\alpha)$ is maximal, with $R/(x-\alpha)\cong\mathbb{C}$, since $R/(x-\alpha)\cong\mathbb{R}[y]/(y^2-1+\alpha^2)\cong\mathbb{C}$. So $P=(x-\alpha)$ is necessarily principal in this case.

(iii) Finally, suppose P is a maximal ideal lying over a maximal ideal P' of codimension 2 in $S=\mathbb{R}[x]$, which must be of the form $P'=(x^2+bx+c)$ with $b^2-4c<0$. Then R/P is a finite extension field of $\mathbb{R}[x]/(x^2+bx+c)\cong\mathbb{C}$, and $R/P\cong\mathbb{C}$. We know P must be the contraction to R of $(x-\alpha, y-\beta)$ for some $\alpha,\beta\in\mathbb{C}$ with $\alpha^2+\beta^2=1$. Here α must satisfy $\alpha^2+b\alpha+c=0$, so $\alpha=-\frac{b}{2}\pm\frac{i}{2}\sqrt{4c-b^2}$. Without loss of generality, we can take the positive square root. (The other choice is conjugate under the Galois group of $\mathbb{C}$ over $\mathbb{R}$, and thus won't change P.) Thus

$$\begin{aligned}\beta^2 &= 1-\alpha^2 = b\alpha+1+c\\ &= -\frac{b^2}{2}+1+c+i\frac{b}{2}\sqrt{4c-b^2}.\end{aligned}\tag{1}$$

There are actually two subcases. Note that $P\cap\mathbb{R}[y]$ must be a maximal ideal in $\mathbb{R}[y]$, hence of codimension 1 or codimension 2. If $P\cap\mathbb{R}[y]=(y-\beta)$ is of codimension 1, then β is real and $b=0$, $0<c$. This case is just like case (ii) above, and $P=(y-\beta)$ is principal. The other subcase is where α and β are both complex, so $P\cap\mathbb{R}[x]$ and $P\cap\mathbb{R}[y]$ are both of codimension 2 (in $\mathbb{R}[x]$, $\mathbb{R}[y]$, respectively). In this case, β is the root of an irreducible quadratic $y^2+b'y+c'$, where $b',c'\in\mathbb{R}$ can be computed explicitly from (1). And P contains both x^2+bx+c and $y^2+b'y+c'$. However, since the images of x and y in R satisfy $x^2+y^2=1$, P also contains $f(x,y)=bx+b'y+c+c'+1$, which is a linear polynomial. We claim that P is just the principal ideal generated by $f(x,y)$. This can be seen by making a linear change of coordinates $x'=(\cos\theta)x+(\sin\theta)y$, $y'=-(\sin\theta)x+(\cos\theta)y$ for suitable θ, to write R as $\mathbb{R}[x',y']/(x'^2+y'^2-1)$, where x' and y' are linear combinations of x and y and (f) is now of the form $(x'-\alpha)$. (Here we're using the fact that the circle is invariant under rotations.) This reduces us to a previous case.

(c) Since the class group of a Dedekind domain is generated by the non-principal prime ideals, we see from (b) that the class group is generated by the prime ideals P of the form $(x-\alpha, y-\beta)$, with $\alpha,\beta\in\mathbb{R}$, $\alpha^2+\beta^2=1$.

(i) Given such a prime ideal P, let's show that P^2 is principal. As above, we may make a linear change of coordinates and suppose that $P=(x-1,y)$ (in the new coordinate system). Then $P^2=((x-1)^2,2(x-1)y,y^2)$. But $y^2=1-x^2=-(x-1)(1+x)$ in R, so all the generators of P^2 are divisible by $x-1$, and $P^2\subseteq(x-1)$. On the other hand, $2(x-1)=(x-1)(x+1)-(x-1)^2\in P^2$, so $(x-1)\subseteq P^2$, and $P^2=(x-1)$ is principal. Thus the image of P in the class group is of order 2.

(ii) Now let's take two distinct non-principal prime ideals P_1 and P_2. As above, we may assume $P_1 = (x-1, y)$, and $P_2 = (x-\alpha, y-\beta)$ with $\alpha, \beta \in \mathbb{R}$, $\alpha^2+\beta^2 = 1$, $\alpha < 1$. The general case works basically the same way, but to simplify the algebra, let's take $\alpha = 0$, $\beta = 1$, so $P_2 = (x, y-1)$. Then $P_1P_2 = ((x-1)x, (x-1)(y-1), xy, y(y-1))$. Then $(x-1)(y-1)-xy = 1-x-y \in P_1P_2$, and we claim that in fact $P_1P_2 = (1-x-y)$. Indeed, $P_1P_2 = ((x-1)x, xy, 1-x-y)$, since $(x-1)(y-1) = xy+(1-x-y)$, and $y(y-1) = (1-x^2)-y = (1-x-y)-x(x-1)$. But $(1-x-y)^2 = 1+x^2+y^2-2x-2y+2xy = 2(1-x-y)+2xy$, so $xy \in (1-x-y)$. Similarly, $(x-1)x = -x(1-x-y)-xy \in (1-x-y)$, since $xy \in (1-x-y)$. Thus all the generators of P_1P_2 lie in $(1-x-y)$, and $P_1P_2 = (1-x-y)$ is principal. Thus the classes of P_1 and of P_2 are each other's inverses in the class group of R.

To summarize, we've shown that all non-principal prime ideals define the same element of the class group, and that the class group is of order 2.

(2) For each of the following $\mathbb{Z}$-modules M, compute the P-adic completion $\widehat{M}$, where $P = (2)$. Does $\widehat{M}$ coincide with $\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} M$? Note: in this problem, $\widehat{\mathbb{Z}}$ is the (2)-adic completion $\widehat{\mathbb{Z}}_{(2)}$ of $\mathbb{Z}$, or in other words, the 2-adic integers.

(a) $M = \mathbb{Z}/(3)$. Since (2) and (3) are relatively prime, $PM = M$, and thus $P^nM = M$ for all n, so $\widehat{M} = \varprojlim M/P^nM = 0$. We have $\widehat{M} \cong \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} M$ since M is finitely generated. One can also check this directly since $\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} M = \widehat{\mathbb{Z}}_{(2)}/(3) = 0$ (3 is a 2-adic unit).

(b) $M = \mathbb{Z}/(2)$. Note $PM = 0$, and thus $P^nM = 0$ for all n, so $\widehat{M} = \varprojlim M/P^nM = M = \mathbb{Z}/(2)$. We have $\widehat{M} \cong \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} M$ since M is finitely generated. One can also check this directly since $\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} M = \widehat{\mathbb{Z}}_{(2)}/(2) = \mathbb{Z}/(2)$.

(c) $M = \mathbb{Q}/\mathbb{Z}$. This is divisible, so $P^nM = M$ for all n and $\widehat{M} = \varprojlim M/P^nM = 0$. On the other hand, $\mathbb{Q}/\mathbb{Z} = \varinjlim C_m$, where C_m is a cyclic group of order m and where C_m embeds in C_n whenever m divides n. So $\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} M = \varinjlim \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} C_m = \varinjlim \widehat{\mathbb{Z}}/(m)$. If $m = 2^r s$, where s is odd, then s is a unit in $\widehat{\mathbb{Z}}$, so $\widehat{\mathbb{Z}}/(m) = \widehat{\mathbb{Z}}/(2^r) = \mathbb{Z}/(2^r)$. Thus the limit is the union of all 2-primary cyclic groups, or $\mathbb{Z}\left[\frac{1}{2}\right]/\mathbb{Z}$, which is NOT the same as $\widehat{M}$.

(d) $M = \mathbb{Q}$. This is divisible, so $P^nM = M$ for all n and $\widehat{M} = \varprojlim M/P^nM = 0$. But $\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$ is a $\mathbb{Q}$-vector space of uncountable dimension.