Math 620, Fall, 1999
Homework Set 2: Dedekind Domains
Solutions to Selected Problems

2. Let $R = \mathbb{Z}[\sqrt{-3}]$, with field of fractions $F = \mathbb{Q}[\sqrt{-3}]$. From the last homework set, R is not integrally closed in F, and hence is not a Dedekind domain. Exhibit a fractional ideal in R that does not have an inverse. Is this fractional ideal a projective R-module?

Solution. Let $I = (2, 1-\sqrt{-3})$, an ideal of R. Let $J = \{x \in F : xI \subseteq R\}$. If I were to be invertible, this would have to be its inverse. Then for $x = a+b\sqrt{-3}$ (a, $b \in \mathbb{Q}$) to lie in J, we have the conditions $2(a+b\sqrt{-3}) \in R$, or $2a \in \mathbb{Z}$ and $2b \in \mathbb{Z}$, and $(1-\sqrt{-3})(a+b\sqrt{-3}) \in R$, or $a+3b \in \mathbb{Z}$ and $b-a \in \mathbb{Z}$. These conditions say exactly that $a = \frac{m}{2}$, $b = \frac{n}{2}$, with m, $n \in \mathbb{Z}$ of the same parity. But then JI is spanned by the $m+n\sqrt{-3}$ and by the $\frac{m+3n}{2} + \frac{m-n}{2}\sqrt{-3}$, with m and n of the same parity. This lattice is spanned by 2, $2\sqrt{-3}$, and $1+\sqrt{-3}$, so it contains 2 but not 1. In particular, $IJ \neq R$, so I is not invertible as a fractional ideal.

Moreover, I can't be a projective R-module either. The reason is simple. If I were projective, then the map of R-modules $R^2 \twoheadrightarrow I$ given by $(x, y) \mapsto 2x + (1-\sqrt{-3})y$ would have to split. The splitting map would have to be given by $x \mapsto (yx, zx)$ for some y, $z \in F$, where yx, $zx \in R$ and $2yx + (1-\sqrt{-3})zx = x$ for $x \in I$. This is another way of saying that I would have to be invertible as a fractional ideal.

4. Let $R = \mathbb{R}[x,y]/(x^2+y^2-1)$, the ring of real-valued polynomial functions on the circle $x^2+y^2 = 1$ in the x-y plane. Show that R is a Dedekind domain. (Hint: Obviously R is Noetherian. Show that every non-zero prime ideal is maximal and that R is integrally closed in its field of fractions.) For extra credit, but hard: See if you can show $C(R)$ has order 2, by finding all the maximal ideals and determining which ones are principal.

Solution. Let $D = \mathbb{R}[x]$, a PID, and let K be its field of fractions $\mathbb{R}(x)$. Note that $y^2 - (1-x^2)$ is irreducible in $K[y]$, so R sits in the field $L = K(\sqrt{1-x^2})$, a Galois extension of K of degree $[L : K] = 2$. Let D' be the integral closure of D in L. Clearly $R \subseteq D'$, and since D' is a Dedekind domain, it is enough to show that $D' \subseteq R$. Let $f + yg \in D'$, where $y^2 = 1-x^2$ and f, $g \in K$. Note that the non-trivial element of $\mathrm{Gal}(L/K)$ sends y to $-y$.

If $g = 0$, then $f \in K \cap D' = D$, since D is a PID and is thus integrally closed. So we may assume $g \neq 0$. Then $f + yg$ has minimal polynomial

$$\begin{aligned}\big(t-(f+yg)\big)\big(t-(f-yg)\big) &= (t-f)^2 - y^2g^2\\ &= t^2 - 2ft + (f^2 - y^2g^2),\end{aligned}$$

and the condition that $f + yg$ be integral over D says that $2f \in D$ and $f^2 - y^2g^2 \in D$. Since $\frac{1}{2} \in \mathbb{R} \subset D$, $f \in D$ and thus $y^2g^2 \in D$, or $(1-x^2)g^2 \in D$. Since the irreducible polynomials $1 \pm x$ only divide $1-x^2$ *once*, they can't divide the denominator of g, since otherwise they would divide the denominator of g^2 *twice* and not cancel out. So $g \in D$, proving that $f + yg \in D[y]/(x^2+y^2-1) = R$. So $R = D'$ is a Dedekind domain.

Now let's classify the maximal ideals of R according to the way the maximal ideals $\mathfrak{p}$ of $D = \mathbb{R}[x]$ split in R. Note that since every irreducible polynomial in $\mathbb{R}[x]$ has degree 2, we have two cases to consider, $\mathfrak{p} = (x - a)$, $a \in \mathbb{R}$, and $\mathfrak{p} = (x^2 + bx + c)$, b, $c \in \mathbb{R}$, $b^2 - 4c < 0$. In the first case, $R/\mathfrak{p}R$ is generated over $D/\mathfrak{p} \cong \mathbb{R}$ by y with $y^2 = 1 - x^2 \equiv 1 - a^2$, so if $|a| > 1$, $R/\mathfrak{p}R \cong \mathbb{C}$, and if $|a| < 1$, $R/\mathfrak{p}R \cong \mathbb{R} \oplus \mathbb{R}$, and if $|a| = 1$, $\mathfrak{p}$ ramifies and $R/\mathfrak{p}R \cong \mathbb{R}[y]/(y^2)$. Thus if $|a| > 1$, the principal ideal $(x - a)$ of R is maximal, and if $|a| < 1$, it splits into two maximal ideals, $(x - a, y - \sqrt{1 - a^2})$ and $(x - a, y + \sqrt{1 - a^2})$, both non-principal. Over $(x+1)$ or $(x-1)$, there is a unique maximal ideal of R, $(x+1, y)$ or $(x - 1, y)$. These are also non-principal.

Now consider the second case, where $\mathfrak{p} = (x^2 + bx + c)$ with $b^2 - 4c < 0$. Then $R/\mathfrak{p}R$ is generated over $D/\mathfrak{p} \cong \mathbb{C}$ by y with $y^2 = 1 - x^2 \equiv 1 + c + bx$. So $R/\mathfrak{p}R \cong \mathbb{C} \oplus \mathbb{C}$ and there are two maximal ideals $\mathfrak{P}$ over $\mathfrak{p}$ in this case, also, corresponding to the two complex square roots of $1 + c + bx$. If $b = 0$ and $c > 0$, then these maximal ideals are generated by $y \pm \sqrt{1 + c}$. Otherwise, x and y *both* map in $R/\mathfrak{P} \cong \mathbb{C}$ to non-real complex numbers, hence for some $d \neq 0$ in $\mathbb{R}$, $x + dy$ maps to a real number e, and $\mathfrak{P}$ turns out to be a principal ideal $(x + dy - e)$, with the line $x + dy - e = 0$ not meeting the circle $x^2 + y^2 = 1$ in the *real* plane $\mathbb{R}^2$.

To summarize, we see that the maximal ideals of R are of two types: principal ideals generated by linear polynomials (corresponding to lines in $\mathbb{R}^2$ not intersecting the unit circle), and non-principal ideals of the form $\mathfrak{P} = (x - a, y - b)$, a, $b \in \mathbb{R}$, where $a^2 + b^2 = 1$. Since every fractional ideal has a unique factorization into maximal ideals, $C(R)$ is generated by the classes of the ideals $\mathfrak{P} = (x - a, y - b)$, a, $b \in \mathbb{R}$, where $a^2 + b^2 = 1$.

Now to show that $C(R)$ is cyclic of order 2, we simply observe that for $\mathfrak{P} = (x-a, y-b)$, $a^2 + b^2 = 1$, $\mathfrak{P}^2 = ((x - a)^2, (y - b)^2, (x - a)(y - b))$. This contains $(x - a)^2 + (y - b)^2 = 2 - 2ax - 2by$ and thus $ax + by - 1$, and it's easy to see that $\mathfrak{P}^2 = (ax + by - 1)$. (Note by the way that the line $ax + by - 1 = 0$ is the tangent line to the unit circle at the point (a, b).) So the class of $\mathfrak{P}$ is of order 2 in $C(R)$. On the other hand, if $\mathfrak{P}_j = (x - a_j, y - b_j)$, $a_j^2 + b_j^2 = 1$, $j = 1$, 2, with $(a_1, b_1) \neq (a_2, b_2)$, then $\mathfrak{P}_1\mathfrak{P}_2$ is the principal ideal generated by the linear polynomial corresponding to the line joining (a_1, b_1) and (a_2, b_2) in $\mathbb{R}^2$. So $\mathfrak{P}_1\mathfrak{P}_2 = \mathfrak{P}_1\mathfrak{P}_2^{-1}$ is trivial in $C(R)$ and $\mathfrak{P}_1$ and $\mathfrak{P}_2$ define the same element of $C(R)$.