Homework 2 Solutions

Dedekind rings are introduced in Lang on page 88. Noetherian rings are discussed in Chapters 4 and 10. We will only need the definitions of both.

Let R be a commutative ring. We recall that R is called a *domain* if $xy=0$ for x, $y \in R$ implies that $x=0$ or $y=0$. A ring R is a domain if and only if it can be embedded in a field. If F is a field containing R, then F is called the *field of fractions* of R if every element of F is of the form x/y with $x, y \in R$ and $y \neq 0$. The field of fractions is uniquely determined up to isomorphism. We will prove all these facts when we consider localization. But for example, the field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$.

If R is a domain and F its field of fractions, then a *fractional ideal* $\mathfrak{a}$ of R is a nonzero, finitely-generated R-submodule of F. We can multiply fractional ideals: $\mathfrak{a}\mathfrak{b}$ is the additive subgroup of F generated by elements ab with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. It is a fractional ideal.

A commutative ring R is called *Noetherian* if every ascending chain of ideals terminates. That is, if $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots$ are ideals, then eventually $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \ldots$ for sufficiently large n.

1. (a) Prove that a principal ideal domain is Noetherian.

(b) Prove that $\mathbb{Z}[\sqrt{-5}]$ is Noetherian.

Solution: (a) If $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots$ is a chain of ideals of the principal ideal domain R, then $\mathfrak{a} = \bigcup \mathfrak{a}_i$ is an ideal. Indeed, to see that it is closed under addition, note that if x, $y \in \mathfrak{a}$ then $x \in \mathfrak{a}_i$ and $y \in \mathfrak{a}_j$ for some i, j. Without loss of generality, $i \leqslant j$, so x, $y \in \mathfrak{a}_j$ and so $x + y \in \mathfrak{a}_j \subseteq \mathfrak{a}$. (It is also clear that $R\mathfrak{a} \subseteq \mathfrak{a}$.) Since R is a principal ideal domain, $\mathfrak{a} = R\alpha$ for some $\alpha \in \mathfrak{a}$. If $\alpha \in \mathfrak{a}_k$ then $\mathfrak{a} \subseteq \mathfrak{a}_k$ proving the ascending chain condition.

(b) Note that $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z} \cdot 1 \oplus \mathbb{Z} \cdot \sqrt{-5}]$ is a finitely generated $\mathbb{Z}$-module. Since $\mathbb{Z}$ is Noetherian, every submodule of this finitely generated module is finitely generated. Thus $R = \mathbb{Z}[\sqrt{-5}]$ is Noetherian as a $\mathbb{Z}$-module, *a fortiori* as an R-module. **Alternative:** Use the Hilbert Basis Theorem (Chapter IV, Theorem 4.1) to see that the polynomial ring $\mathbb{Z}[X]$ is Noetherian. Let p: $\mathbb{Z}[X] \longrightarrow \mathbb{Z}[\sqrt{-5}]$ be the map $f(X) \mapsto f(\sqrt{-5})$. If $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$ is an ascending chain of ideals in $\mathbb{Z}[\sqrt{-5}]$ then $p^{-1}(\mathfrak{a}_1) \subseteq p^{-1}(\mathfrak{a}_2) \subseteq \cdots$ is an ascending chain of ideals in $\mathbb{Z}[X]$, hence it must terminate. This implies that the chain $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$ terminates.

2. Assume that R is a Noetherian domain.

(a) Prove that a nonzero R-submodule of F is a fractional ideal if and only if $\mathfrak{a} \subseteq cR$ for some $c \in F$.

(b) Prove that a principal ideal domain is a Dedekind ring.

Solution: (a) First assume that $\mathfrak{a}$ is a fractional ideal. By hypothesis it is finitely generated. Let a_i/b_i $(i=1,\cdots,n)$ be the generators, and let $b=\prod b_i$ be the common denominator. The $b\mathfrak{a}\subseteq R$ so $\mathfrak{a}\subseteq cR$ with $c=1/b$. Conversely, if $\mathfrak{a}\subseteq cR$ then $c^{-1}\mathfrak{a}$ is an ideal, finitely generated since R is Noetherian. Since $\mathfrak{a}\cong c^{-1}\mathfrak{a}$ as an R-module it is also finitely generated.

(b) Let F be the field of fractions of the principal ideal domain R.

Lemma 1. *Every fractional ideal of the principal ideal domain is of the form dR for some $d\in F^\times$.*

Proof. By part (a), a fractional ideal $\mathfrak{a}$ is contained in cR for $c\in F$. Write $c=a/b$ with $a,b\in R$. Then $b\mathfrak{a}\subseteq aR$, so $b\mathfrak{a}$ is an ideal. Thus $b\mathfrak{a}=tR$ for some $t\in R$ because R is a PID. Thus $a=dR$ with $d=t/a$. □

Now a fractional ideal is invertible since $d^{-1}R$ will serve as an inverse to dR. The set $\mathfrak{P}$ of fractional ideals thus forms a group. Since $d\mapsto dR$ is a homomorphism from $F^\times\longrightarrow\mathfrak{P}$ which is surjective (by the Lemma) with kernel $R^\times$, the multiplicative group of R, we see that $\mathfrak{P}\cong F^\times/R^\times$.

3. **An example of an ideal in a Dedekind ring that is not principal.** Let $R=\mathbb{Z}[\sqrt{-5}]$. It may be shown that R is a Dedekind ring. Let

$$I=\{a+b\sqrt{-5}|a,b\in\mathbb{Z},\, a\equiv b \bmod 2\}.$$

The exercise will show that this ideal is not principal.

(a) Let $R^*=R-\{0\}$ and $I^*=I-\{0\}$. (Some authors use R^* for the multiplicative group of units of a ring R, but I will use $R^\times$ for that.) Observe that if $N\colon R\longrightarrow\mathbb{Z}$ is the map $N(z)=|z|^2$, so $N(a+b\sqrt{-5})=a^2+5b^2$, then $N(zw)=N(z)\ N(w)$. So $N(R^*)$ and $N(I^*)$ are multiplicative monoids contained in $\mathbb{Z}$. Show that the smallest two nonzero elements of $N(I^*)$ are 4 and 6, while the smallest nonzero elements of $N(R^*)$ are 1 and 4.

(b) Use (a) to show that I is not a principal ideal.

(c) Prove that I is a maximal ideal. (Hint: what is the index $[R\colon I]$ as abelian groups?)

(d) To prove that R is a Dedekind domain we need to know that every fractional ideal is invertible. We will not prove this right now, but show that $I^2=2R$ and deduce that I is invertible.

Solution. (a) Since $N(a+b\sqrt{-5})=a^2+5b^2$ we have $N(a+b\sqrt{-5})>4$ if $b\neq 0$. Therefore $1=N(1)$ and $4=N(2)$ are the smallest possible norms of elements of R. On the other hand if $a+b\sqrt{-5}$ is known to be in I then a and b are either both even or both odd, so 1 is not a norm; the smallest norms in this case are $4=N(2)$ and $6=N(1+\sqrt{-5})$.

(b) If the ideal I were principal, say $I=R\alpha$, then the norms of elements of I would be $A=N(\alpha)$ times the norms of elements of R, and the two smallest norms would be A and $4A$. No choice of A makes these into 4 and 6.

(c) Observe that I has index two in R. Indeed if $x \notin I$ then $x-1 \in I$ and so R/I has only two cosets. If J is an ideal between I and R, that is $R \supset J \supset I$ then $2=[R\colon I]=[R\colon J][J\colon I]$ so either $[R\colon J]=1$ or $[J\colon I]=1$, i.e. $J=R$ or I. This shows that I is maximal. **Alternative:** Since $[R\colon I]=2$, the quotient ring R/I has only two elements and is clearly a field. Since R/I is a field, I is maximal.

(d) Note that $2=(1+\sqrt{-5})(1-\sqrt{-5})-2\cdot 2 \in I\cdot I$. Therefore $2R \subseteq I^2$. On the other hand, I^2 is generated by elements of the form

$$(a+b\sqrt{-5})(c+d\sqrt{-5})=A+B\sqrt{-5}, \qquad A=ac-5bd, \quad B=ac+bd$$

where $a \equiv b \bmod 2$ and $c \equiv d \bmod 2$. We claim that A and B are both even. If a and b are both even or if c and d are both even, this is obvious, so assume a, b, c, d are all odd. Then ac and $5bd$ are odd so A is even, and similarly B. This proves the converse inequality $I^2 \subset 2R$.

4. **An example of an ideal that is projective but not free**. Notations will be as in the last problem.

(a) Prove that I is not a free module.

(b) Define $f\colon R\oplus R \longrightarrow I\oplus I$ be multiplication by the matrix

$$M=\begin{pmatrix} 1+\sqrt{-5} & 2 \\ 2 & 1-\sqrt{-5} \end{pmatrix}.$$

Show that f is an isomorphism $R\oplus R \longrightarrow I\oplus I$. Conclude that I is a projective module.

Solution. For (a), note that any two elements x, y of I cannot be linearly independent over R since their ratio lies in the field $\mathbb{Q}(\sqrt{-5})$ of fractions, so $x/y=\alpha/\beta$ with $\alpha, \beta \in R$ and so $\alpha x-\beta y=0$. This means that if I is free, it is free of rank one. Thus as an ideal, it is principal, contradicting Problem 3.

(b) Since the entries of M are in I, the map f takes $R\oplus R$ into $I\oplus I$. As for the inverse map,

$$M^{-1}=\frac{1}{2}\begin{pmatrix} 1-\sqrt{-5} & -2 \\ -2 & 1+\sqrt{-5} \end{pmatrix}.$$

Note that the coefficients are in $\frac{1}{2}I$. So applying this to $I\oplus I$ produces elements of $\frac{1}{2}I^2 \oplus \frac{1}{2}I^2 = R\oplus R$ by Problem 3(d). Hence $f\colon I\oplus I \longrightarrow R\oplus R$ is a bijection. We see that $I\oplus I$ is free. Since it is a summand in a free module, it is projective.