Math 210B: Homework 4 Solutions

All rings are commutative, with 1. Some of the problems make use of the norm map, so review Theorem VI.5.1 of Lang's *Algebra*.

We will say a ring is of *dimension 1* if it is not a field and every nonzero prime ideal is maximal. Recall that a Dedekind domain is an integral domain that is integrally closed (meaning integrally closed in its field of fractions), Noetherian, and of dimension 1.

Problem 1. Let E/F be a finite separable field extension and let $N : E^\times \to F^\times$ be the norm map. Let A be a subring of F that is integrally closed (in F) and let B be the integral closure of A in E. Let $x \in B$. Show that $N(x) \in A$. Moreover show that $x \in B^\times$ if and only if $N(x) \in A^\times$.

Solution. Let $\sigma_i : E \to \overline{F}$ be the distinct embeddings of E into the algebraic closure over F. If $x \in B$ then $N(x) = \prod_i \sigma_i(x)$, where each $\sigma_i(x)$ is integral over A. Thus $N(x) \in F$ and $N(x)$ is integral over A. Since A is integrally closed, $N(x) \in A$.

If x is a unit in B, write $1 = xy$ for $y \in B$. Then $1 = N(1) = N(x)N(y)$ so $N(x)$ is a unit.

Conversely, suppose that $N(x)$ is a unit. Order the embeddings σ_i so that σ_1 is the identity and consider $y = \prod_{i \neq 1} \sigma_i(x)$. This is integral over A since each $\sigma_i(x)$ is. Moreover $y = N(x)/x \in E$ since $x, N(x) \in E$. Since B is the integral closure of A in E, $y \in B$. Now $N(x) = xy$ is a unit by assumption and $y \in B$, so x must be a unit.

Problem 2. Let E/F be a finite separable field extension and let A be a Dedekind domain whose field of fractions is F. Let B be the integral closure of A in E. Prove that B is a Dedekind domain.

Solution. Clearly B is integrally closed, and it is Noetherian by Problem 5 of Homework 3.

We show that B is of dimension 1. Let $\mathfrak{P}$ be a maximal ideal of B. We will argue that $\mathfrak{P} \cap A$ is nonzero. Let $\sigma_1, \cdots, \sigma_r$ be the distinct embeddings over F of E into the algebraic closure $\overline{F}$ of F. We order them so that σ_1 is the identity map. Let x be a nonzero element of $\mathfrak{P}$. We will show that $N(x) = \prod \sigma_i(x)$ is a nonzero element of $\mathfrak{P} \cap A$. Indeed, $N(x)$ is a nonzero element of F by Theorem VI.5.1 on page 285 of Lang. It is integral over A since the $\sigma_i(x)$ satisfy the same monic polynomial in $A[x]$ as x. Since A is integrally closed, $N(x) \in A$. We will show that it is in $\mathfrak{P}$. First note that $N(x)/x \in E$ since $N(x) \in F$ and $x \in E$. Since $N(x)/x = \prod i \neq 1 \sigma_i(x)$ it is integral over A and hence $N(x)/x \in B$. Therefore $N(x) = x \cdot (N(x)/x) \in \mathfrak{P}$. We have shown that $N(x) \in \mathfrak{P} \cap A$, so this is a nonzero ideal of A. It is prime since $\mathfrak{P}$ is prime. Since A is a Dedekind domain, $\mathfrak{P} \cap A$ is maximal. Then $\mathfrak{P}$ is maximal by Lang, Proposition VII.1.11 on page 339. This proves that B is of dimension 1.

Problem 3. Show that a principal ideal domain is a Dedekind domain. Show that $\mathbb{Z}[\sqrt{-5}]$ is Dedekind domain that is not a PID.

Solution. $\mathbb{Z}[\sqrt{-5}]$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-5})$ by Problem 4 of Homework 1, so it is a Dedekind domain by the last problem. To show that it is not a principal ideal domain, let

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

It is easy to see that $\mathfrak{a}$ is an ideal. We argue that $\mathfrak{a}$ is not principal. If $\mathfrak{a} = (\alpha)$, then 2 and $1 + \sqrt{-5}$ are both multiples of α. Thus $4 = N(2)$ and $6 = N(1 + \sqrt{-5})$ are both multiples of $N(\alpha) \in \mathbb{Z}$. This implies that $N(\alpha) = \pm 1$, which implies that $\alpha = \pm 1$, a contradiction since $\mathfrak{a} \neq (1)$.

Let $\mathfrak{o}$ be a Dedekind domain and let K be its field of fractions. Let $\mathfrak{a}$ be a nonzero $\mathfrak{o}$-submodule of K. If there exists $c \in \mathfrak{o}$ such that $c\mathfrak{a} \subset \mathfrak{o}$, then $\mathfrak{a}$ is called a *fractional ideal*. Thus a nonzero ideal of $\mathfrak{o}$ is a fractional ideal.

The next exercise continues (from Homework 3) Exercise VII.7 in Lang's *Algebra.*

Problem 4. Let $\mathfrak{o}$ be a Dedekind domain and let K be its field of fractions. Let $\mathfrak{p}$ be a maximal ideal of K. Define

$$\mathfrak{p}^{-1} = \{x \in K | x\mathfrak{p} \subseteq \mathfrak{o}\}.$$

(a) Show that $\mathfrak{p}^{-1}$ is a fractional ideal containing $\mathfrak{o}$ and that $\mathfrak{p}^{-1} \neq \mathfrak{o}$.

(b) Continuing from the preceding problem, show that $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{o}$.

(c) Prove that every non-zero ideal is invertible by a fractional ideal. Deduce that the fractional ideals of $\mathfrak{o}$ form a group under multiplication.

Hints: For (a) try to use Problem 6 from Homework 3. If $0 \neq x \in \mathfrak{p}$ show that you can find primes $\mathfrak{p}_i$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq x\mathfrak{o} \subseteq \mathfrak{p}$. Show that one of the $\mathfrak{p}_i = \mathfrak{p}$. Then what? For (b), use the assumption that $\mathfrak{o}$ is integrally closed to rule out the possibility that $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$.

Solution. For (a), let us show that $\mathfrak{p}^{-1}$ is a fractional ideal. Indeed, pick a nonzero element c of $\mathfrak{p}$ and note that $c\mathfrak{p}^{-1} \subseteq \mathfrak{o}$ by definition of $\mathfrak{p}^{-1}$. The hard part will be to show that $\mathfrak{p}^{-1}$ is strictly larger than $\mathfrak{o}$. Let $x \in \mathfrak{p}$ and using (a) find maximal ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ such that $(x) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Take r minimal for this. We claim $\mathfrak{p}$ must be one of the $\mathfrak{p}_i$. If not, then $\mathfrak{p}_i \neq \mathfrak{p}$ so we can find $x_i \in \mathfrak{p}_i \backslash \mathfrak{p}$. Then

$$\prod x_i \in \prod \mathfrak{p}_i \subseteq (x) \subseteq \mathfrak{p}$$

but $x_i \notin \mathfrak{p}$, which is a contradiction because $\mathfrak{p}$ is prime. Reordering the $\mathfrak{p}_i$ we may assume that $\mathfrak{p}_1 = \mathfrak{p}$. Now

$$\mathfrak{p} \supseteq (x) \supseteq \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r$$

and by the minimality of r we have $(x) \not\supseteq \mathfrak{p}_2 \cdots \mathfrak{p}_r$. Now the map $\mathfrak{a} \mapsto x\mathfrak{a}$ takes fractional ideals to fractional ideals and since it has an inverse $\mathfrak{a} \mapsto x^{-1}\mathfrak{a}$ it is a bijection of the fractional ideals. Thus

$$\mathfrak{o} \supseteq \mathfrak{p} \cdot x^{-1}\mathfrak{p}_2 \cdots \mathfrak{p}_r, \qquad \mathfrak{o} \not\supseteq x^{-1}\mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

This means that we can find an element $y \in x^{-1}\mathfrak{p}_2 \cdots \mathfrak{p}_r$ such that $y \notin \mathfrak{o}$. Then $y \in \mathfrak{p}^{-1}$ proving that $\mathfrak{p}^{-1} \neq \mathfrak{o}$.

(b) From the definition of $\mathfrak{p}^{-1}$ it is clear that $\mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{o}$ and since $\mathfrak{o} \subseteq \mathfrak{p}^{-1}$ we have

$$\mathfrak{o} \supseteq \mathfrak{p}\mathfrak{p}^{-1} \supseteq \mathfrak{p}.$$

Thus either $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}$ or $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. We must rule out the second case. Let $x \in \mathfrak{p}^{-1} \backslash \mathfrak{o}$. Suppose that $x\mathfrak{p} \subseteq \mathfrak{p}$. Then $\mathfrak{p}$ is a faithful $\mathfrak{o}[x]$-module that is finitely generated as an $\mathfrak{o}$-module because $\mathfrak{o}$ is Noetherian. Therefore by the integrality criterion x is integral over $\mathfrak{o}$. But $\mathfrak{o}$ is integrally closed in K, so $x \in \mathfrak{o}$ which is a contradiction.

(c) Suppose that there is a fractional ideal $\mathfrak{a}$ such that $\mathfrak{a}\mathfrak{b} = \mathfrak{o}$ does not have a solution $\mathfrak{b}$ that is a fractional ideal. Since $\mathfrak{o}$ is Noetherian, let $\mathfrak{a}$ be a maximal such counterexample. Let $\mathfrak{p}$ be a maximal ideal containing in $\mathfrak{a}$. Then

$$\mathfrak{a} = \mathfrak{o}\mathfrak{a} \subseteq \mathfrak{p}^{-1}\mathfrak{a} \subseteq \mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{o}$$

so $\mathfrak{p}^{-1}\mathfrak{a}$ is an ideal containing $\mathfrak{a}$. We will show that $\mathfrak{p}^{-1}\mathfrak{a}$ is strictly larger than $\mathfrak{a}$. If not, $\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{a}$ and by the integrality criterion, this means every element of $\mathfrak{p}^{-1}$ is integral over $\mathfrak{o}$, which we know is not true. By maximality of the counterexample $\mathfrak{a}$ we have $\mathfrak{c}\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{o}$ for some fractional ideal $\mathfrak{c}$ and so $\mathfrak{a}\mathfrak{b} = \mathfrak{o}$ with $\mathfrak{b} = \mathfrak{c}\mathfrak{p}^{-1}$.

Now it is clear that fractional ideals form a multiplicative monoid, and (d) shows that elements are invertible, so fractional ideals form a group.

Problem 5. Let R be a principal ideal domain with a unique nonzero prime ideal. Prove that R is a valuation ring of its field of fractions F.

We will call a principal ideal domain with a unique nonzero prime ideal a *discrete valuation ring* (DVR).

Solution. Let $\mathfrak{p}$ be the unique maximal ideal. It is principal, so write $\mathfrak{p} = \varpi R$. If $a \in F$ write $a = b/c$ with $b, c \in R$. Since a PID is a UFD we may write $b = \varpi^n \beta$ and $c = \varpi^m \gamma$ with β, γ units. Then $a = \varpi^{n-m}\alpha$ where $\alpha = \beta/\gamma \in R^\times$. If $n \geqslant m$ then $a \in R$, while if $n \leqslant m$, then $1/a \in R$. This proves that R is a valuation ring.