# Commutative Algebra Homework 8

Michael Nelson

## Problem 1

**Exercise 1.** Let $R$ be a Dedekind domain and let $I$ be an ideal of $R$. Show that $I$ can be generated by two elements.

**Solution 1.** Write $I = \prod_{i=1}^r \mathfrak{p}_i^{a_i}$ where $\mathfrak{p}_i$'s are pairwise distinct prime ideals and where the $a_i$ are nonnegative integers. Let $\alpha \in I$. If $I = \langle \alpha \rangle$ then we are done, so assume $\langle \alpha \rangle \subset I$ where the inclusion is strict. Since $\langle \alpha \rangle \subset I$, the prime factorization of $\langle \alpha \rangle$ must have the form

$$\langle \alpha \rangle = \prod_{i=1}^r \mathfrak{p}_i^{b_i} \prod_{j=1}^s \mathfrak{q}_j^{d_j},$$

where the $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are all pairwise relatively prime, where $b_i \geq a_i$ for each $i$, and where $d_j$ is a nonnegative integer for each $j$. For each $i$, choose $\beta_i \in \mathfrak{p}_i^{a_i} \backslash \mathfrak{p}_i^{a_i+1}$. Note that $\mathfrak{p}_i$ and $\mathfrak{q}_j$ being relatively prime implies $\mathfrak{p}_i^{a_i+1}$ and $\mathfrak{q}_j$ are relatively prime. Thus by the Chinese Remainder Theorem, we can find a $\beta \in R$ such that

$$\beta \equiv \beta_i \bmod \mathfrak{p}_i^{a_i+1} \quad \text{and} \quad \beta \equiv 1 \bmod \mathfrak{q}_j$$

for all $i$ and $j$. In particular, $\beta \in \mathfrak{p}_i^{a_i} \backslash \mathfrak{p}_i^{a_i+1}$ for all $i$ and $\beta \notin \mathfrak{q}_j$ for all $j$. Indeed, it is clear that $\beta \notin \mathfrak{q}_j$ since $\beta \equiv 1 \bmod \mathfrak{q}_j$ for all $j$. To see that $\beta \in \mathfrak{p}_i^{a_i} \backslash \mathfrak{p}_i^{a_i+1}$ for all $i$, observe that $\beta \equiv \beta_i \bmod \mathfrak{p}_i^{a_i+1}$ implies $\beta = \beta_i + \alpha_i$ for some $\alpha_i \in \mathfrak{p}_i^{a_i+1}$. Thus clearly $\beta \in \mathfrak{p}_i^{a_i}$. If $\beta \in \mathfrak{p}_i^{a_i+1}$, then since $\beta_i = \alpha_i - \beta$, we would then have $\beta_i \in \mathfrak{p}_i^{a_i+1}$, which is a contradiction.

Note that since $\beta \in \mathfrak{p}_i^{a_i}$ for all $i$, we have

$$\begin{aligned} \beta &\in \bigcap_{i=1}^r \mathfrak{p}_i^{a_i} \\ &= \prod_{i=1}^r \mathfrak{p}_i^{a_i} \\ &= I. \end{aligned}$$

Thus the prime factorization of $\langle \beta \rangle$ must have the form

$$\langle \beta \rangle = \prod_{i=1}^r \mathfrak{p}_i^{c_i} \prod_{k=1}^t \widetilde{\mathfrak{q}}_k^{e_k},$$

where the $\mathfrak{p}_i$ and $\widetilde{\mathfrak{q}}_k$ are all pairwise relatively prime, where $c_i \geq a_i$ for each $i$, and where $e_k$ is a nonnegative integer for each $j$. However note that we must have $c_i \leq a_i$ since $\beta \notin \mathfrak{p}_i^{a_i+1}$ for each $i$ and we cannot have $\mathfrak{q}_j = \widetilde{\mathfrak{q}}_k$ for some $j$ and $k$ since $\beta \notin \mathfrak{q}_j$ for all $j$. It follows that

$$\begin{aligned} \langle \alpha, \beta \rangle &= \prod_{i=1}^r \mathfrak{p}_i^{\min(b_i, c_i)} \prod_{j=1}^s \mathfrak{q}_j^{\min(d_j, 0)} \prod_{k=1}^t \widetilde{\mathfrak{q}}_k^{\min(0, e_k)} \\ &= \prod_{i=1}^r \mathfrak{p}_i^{\min(b_i, a_i)} \prod_{j=1}^s \mathfrak{q}_j^{\min(d_j, 0)} \prod_{k=1}^t \widetilde{\mathfrak{q}}_k^{\min(0, e_k)} \\ &= \prod_{i=1}^r \mathfrak{p}_i^{a_i} \prod_{j=1}^s \mathfrak{q}_j^{0} \prod_{k=1}^t \widetilde{\mathfrak{q}}_k^{0} \\ &= \prod_{i=1}^r \mathfrak{p}_i^{a_i} \\ &= I. \end{aligned}$$

# Problem 7

## Problem 2

**Exercise 2.** Let $d \in \mathbb{Z}\backslash\{0,1\}$ be squarefree, let $K = \mathbb{Q}(\sqrt{d})$, let $\mathcal{O}_K$ be the integral closure of $\mathbb{Z}$ in $K$, and let $\gamma = (1+\sqrt{d})/2$. Then show that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2,3 \bmod 4 \\ \mathbb{Z}[\gamma] & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

**Solution 2.** Clearly $\sqrt{d} \in \mathcal{O}_K$ since it is a root of the monic $X^2 - d$. Thus $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$. We first want to show that either $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ or $\mathcal{O}_K = \mathbb{Z}[\gamma]$ depending on the congruence class of $d$ modulo 4. Let $\alpha \in \mathcal{O}_K$ and express it as $\alpha = a + b\sqrt{d}$ for unique $a, b \in \mathbb{Q}$. Note that both rational numbers

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \alpha + \overline{\alpha} \quad \text{and} \quad \mathrm{N}_{K/\mathbb{Q}}(\alpha) = \alpha\overline{\alpha}$$

are algebraic integers and thus must belong to $\mathbb{Z}$. Given that $\overline{\alpha} = a - b\sqrt{d}$, a quick computation gives us $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 2a$ and $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = a^2 - db^2$. It follows that $2a \in \mathbb{Z}$ and $a^2 - db^2 \in \mathbb{Z}$. In particular, $2a \in \mathbb{Z}$ implies either $a \in \mathbb{Z}$ or $a = n/2$ where $n$ is an odd integer.

**Case 1:** First assume that $a \in \mathbb{Z}$. Then since $a^2 - db^2 \in \mathbb{Z}$, we see that $db^2 \in \mathbb{Z}$. But $d$ is squarefree, so integrality $db^2$ tells us that we cannot have a prime $p$ occuring in the denominator of $b$ as a reduced-form fraction (we would not be able to cancel the denominator factor $p^2$ for $b^2$). It follows that $b \in \mathbb{Z}$, so $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.

**Case 2:** Assume that $a = n/2$ for some integer $n$. Thus, $a^2 - db^2 = n^2/4 - db^2$ is an integer. In particular we have $db^2 = n^2/4 + k$ for some $k \in \mathbb{Z}$. Observe that

$$\begin{aligned} db^2 &= \frac{n^2}{4} + k \\ &= \frac{n^2 + 4k}{4}. \end{aligned}$$

Since $n$ is odd, it follows that $n^2 + 4k$ is odd, and thus $db^2$ must have a denominator of 4 when written in reduced form. Again, since $d$ is squarefree, it follows that $b = m/2$ for some odd integer $m$. Thus we can write

$$\gamma = \left(\frac{n-1}{2} + \frac{m-1}{2}\sqrt{d}\right) - \alpha$$

with $(n-1)/2 \in \mathbb{Z}$ and $(m-1)/2 \in \mathbb{Z}$. In particular, we have $\gamma \in \mathcal{O}_K$

Thus in either case, we see that $\mathcal{O}_K \subseteq \mathbb{Z}[\gamma]$. In fact, combining these two cases together tells us $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ if and only if $\gamma \notin \mathcal{O}_K$. Indeed, clearly if $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$, then $\gamma \notin \mathcal{O}_K$. Conversely, if $\gamma \notin \mathcal{O}_K$ then every $a + b\sqrt{d} \in \mathcal{O}_K$ must have $a \in \mathbb{Z}$ (otherwise we would get $\gamma \in \mathcal{O}_K$ by case 2, a contradiction), and thus by case 1, every $a + b\sqrt{d} \in \mathcal{O}_K$ belongs to $\mathbb{Z}[\sqrt{d}]$.

Now note that $\gamma \in \mathcal{O}_K$ if and only if $d \equiv 1 \bmod 4$. Indeed, if $\gamma \in \mathcal{O}_K$, then $(1-d)/4 = \mathrm{N}_{K/\mathbb{Q}}(\gamma) \in \mathbb{Z}$, which is equivalent to $d \equiv 1 \bmod 4$. Conversely, if $d \equiv 1 \bmod 4$, then we have $d = 1 + 4k$ for some $k \in \mathbb{Z}$. Thus

$$\begin{aligned} \gamma^2 &= \left(\frac{1+\sqrt{d}}{2}\right)^2 \\ &= \frac{1 + d + 2\sqrt{d}}{4} \\ &= \frac{2 + 4k + 2\sqrt{d}}{4} \\ &= \frac{1 + 2k + \sqrt{d}}{2} \\ &= \frac{1+\sqrt{d}}{2} + k. \\ &= \gamma + k \end{aligned}$$

It follows that $\gamma \in \mathcal{O}_K$. Thus

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2,3 \bmod 4 \\ \mathbb{Z}[\gamma] & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

## Problem 3

**Exercise 3.** Let $R$ be a domain with quotient field $K$. We say $\omega \in K$ is **almost integral** over $R$ if there is a nonzero $a \in R$ such that $a\omega^n \in R$ for all $n \in \mathbb{N}$. We say that $R$ is completely integrally closed if it contains all of its almost integral elements.

1. Show that if $\omega \in K$ is integral, then $\omega$ is almost integral over $R$.
2. Show that if $R$ is Noetherian and $\omega \in K$ is almost integral over $R$, then $\omega$ is integral over $R$.
3. Given an example of a domain $R$ and an element $\omega \in K$ (where $K$ is the quotient field of $R$) that is almost integral over $R$, but not integral over $R$.
4. Show that any UFD is completely integrally closed.

**Solution 3.** 1. Let $\omega \in K$ be integral over $R$. Write $\omega = a/b$ where $a, b \in R$ with $b \neq 0$. Choose $k \geq 1$ minimal and $a_0, a_1, \dots, a_{k-1} \in R$ such that

$$\omega^k + a_{k-1}\omega^{k-1} + \cdots + a_1\omega + a_0 = 0. \tag{1}$$

We claim that for any for any $n \geq 0$, we have $b^k\omega^n \in R$. Indeed, first note that if $n > k$, then we can use the fact that $\omega$ is integral (so $R[\omega] = \sum_{i=0}^{k-1} R\omega^i$) to write

$$\omega^n = a_{k-1,n}\omega^{k-1} + \cdots + a_{1,n}\omega + a_{0,n}$$

for some $a_{0,n}, a_{1,n}, \dots, a_{k-1,n} \in R$, so it suffices to show that $b^k\omega^n \in R$ when $n \leq k$. This is clear though since

$$\begin{aligned} b^k\omega^n &= b^k\frac{a^n}{b^n} \\ &= b^{k-n}a^n \\ &\in R. \end{aligned}$$

It follows that $\omega$ is almost integral over $R$.

2. Suppose $R$ is a Noetherian domain and let $\omega \in K$ be almost integral over $R$. Choose $a \in R\backslash\{0\}$ such that $a\omega^n \in R$ for all $n \in \mathbb{N}$. Consider the ascending chain of ideals $(I_n)$ where

$$\begin{aligned} I_0 &= \langle a \rangle \\ I_1 &= \langle a, a\omega \rangle \\ &\vdots \\ I_n &= \langle a, a\omega, \dots, a\omega^n \rangle \\ &\vdots \end{aligned}$$

for all $n \in \mathbb{N}$. The ascending chain of ideals $(I_n)$ must terminate since $R$ is Noetherian, say at $m \in \mathbb{N}$. It follows that $a\omega^{m+1} \in I_m$, which implies

$$a\omega^{m+1} = a_m a\omega^m + \cdots + a_1 a\omega + a_0 a \tag{2}$$

for some $a_0, a_1, \dots, a_m \in R$. Canceling $a$ from both sides of (**??**) (we can do this since $A$ is a domain) and rearranging terms gives us

$$\omega^{m+1} - a_m\omega^m - \cdots - a_1\omega - a_0 = 0.$$

This implies $\omega$ is integral over $R$.

3. Consider ring $A = K[y, \{x/y^n \mid n \in \mathbb{N}\}]$. We have a strict inclusion of rings

$$K[x, y] \subset A \subset K[x, y, 1/y].$$

In particular, $A$ is a domain with fraction field $K(x, y)$. Note that $1/y \in K(x, y)$ is almost integral over $A$ since $1/y \notin A$ and $x/y^n \in A$ for all $n \in \mathbb{N}$. On the other hand, $1/y$ is not integral over $A$. Indeed, if it were, then there would exists $m \in \mathbb{N}$ and $f_0, \dots, f_{m-1} \in A$ such that

$$\frac{1}{y^m} = \frac{f_{m-1}}{y^{m-1}} + \cdots + \frac{f_1}{y} + f_0. \tag{3}$$

Multilpying $y^m$ on both sides of (**??**) gives us

$$1 = (f_{m-1} + \cdots + f_1 y^{m-2} + f_0 y^{m-1})y. \tag{4}$$

Evaluating $x = 0$ to both sides of (**??**) gives us

$$1 = (\widetilde{f}_{m-1} + \cdots + \widetilde{f}_1 y^{m-2} + \widetilde{f}_0 y^{m-1})y. \tag{5}$$

where $\widetilde{f}_0, \widetilde{f}_1, \ldots, \widetilde{f}_{m-1}$ are polynomials over $K$ in the variable $y$. Evaluating $y = 0$ to both sides of (**??**) gives us $1 = 0$, which is a contradiction.

4. Let $R$ be a UFD, let $K$ denote its fraction field, and let $\omega \in K$ be almost integral over $R$. Choose a nonzero $a \in R$ such that $a\omega^n \in R$ for all $n \in \mathbb{N}$.