Commutative Algebra Homework 5

Michael Nelson

Problem 1

Definition 0.1. Let R be an integral domain with identity and suppose $x, y \in R \backslash \{0\}$. We say x and y have a **greatest common divisor** if there exists a $d \in R$ which satisfies the following two properties:

1. $d \mid x$ and $d \mid y$,
2. if there exists $d' \in R$ such that $d' \mid x$ and $d' \mid y$, then $d' \mid d$.

If such a d exists, then using the fact that R is a domain, it is easy to see that the set of all greatest common divisors of x and y is $\{ud \mid u \in R^\times\}$. Indeed, d and d' are greatest common divisors of x and y if and only if $d \mid d'$ and $d' \mid d$ if and only if $d' = ud$ for some $u \in R^\times$. If a greatest common divisor of x and y exists, then we often choose one of their greatest common divisors and denote it by $\gcd(x, y)$. Thus $\gcd(x, y)$ is well-defined up to a unit. If we write $\gcd(x, y) = \gcd(x', y')$, then it is understood that this means $\gcd(x, y) \mid \gcd(x', y')$ and $\gcd(x', y') \mid \gcd(x, y)$. We say R is a **GCD domain** if every pair of nonzero elements in R has a greatest common divisor.

Exercise 1. Let R be a GCD domain and let $a, b, c, x \in R$ be nonzero. Show the following.

1. $\gcd(ax, bx) = x \gcd(a, b)$
2. if $d = \gcd(a, b)$, then $\gcd(a/d, b/d) = 1$.
3. If $\gcd(x, a) = \gcd(x, b) = 1$, then $\gcd(x, ab) = 1$.
4. If $\gcd(x, a) = 1$ and x divides ab, then x divides b.
5. Show that R is integrally closed.
6. Show that R is Bezout if and only if $\gcd(a, b)$ is a linear combination of a and b.

Solution 1. 1. Let $d = \gcd(a, b)$ and let $e = \gcd(ax, bx)$. Write

$$\begin{aligned} a_1 d &= a \\ b_1 d &= b \\ a_2 e &= ax \\ b_2 e &= bx \end{aligned}$$

where $a_1, a_2, b_1, b_2 \in R$. Then observe that $a_1 xd = ax$ and $b_1 xd = bx$ implies $xd \mid ax$ and $xd \mid bx$. Since e is the greatest common divisor of ax and bx, it follows that $xd \mid e$. Thus we have $yxd = e$ for some $y \in R$. In particular, note that $e/x = dy \in R$. Next observe that $a_2(e/x) = ax/x = a$ and $b_2(e/x) = bx/x = b$ implies $(e/x) \mid a$ and $(e/x) \mid b$. Since d is the greatest common divisor of a and b, it follows that $d \mid (e/x)$, and hence $dx \mid e$. Since both $dx \mid e$ and $e \mid dx$, we see that $e = dx$.

2. Let $e = \gcd(a/d, b/d)$. By 1, we have

$$\begin{aligned} de &= d \gcd(a/d, b/d) \\ &= \gcd(d(a/d), d(b/d)) \\ &= \gcd(a, b) \\ &= d. \end{aligned}$$

Since $d \neq 0$, it follows that $e = 1$ since R is a domain.

3. Let $d = \gcd(x, ab)$. Since $d \mid x$ and $d \mid ab$, we see that in particular, we have $d \mid xb$ and $d \mid ab$. Since

$$\begin{aligned}\gcd(xb, ab) &= b\gcd(x, a)\\ &= b \cdot 1\\ &= b,\end{aligned}$$

it follows that $d \mid b$. Thus $d \mid x$ and $d \mid b$. Since $\gcd(x, b) = 1$, it follows that $d \mid 1$. Since we already have $1 \mid d$, we see that $\gcd(x, ab) = 1$.

4. We have

$$\begin{aligned}\gcd(xb, ab) &= b\gcd(x, a)\\ &= b \cdot 1\\ &= b,\end{aligned}$$

Thus if $x \mid ab$, then since already $x \mid xb$, we see that $x \mid b$.

5. Let K be the field of fractions of R and let $c/d \in K^\times$ where we may assume that $\gcd(c, d) = 1$. Indeed, if $\gcd(c, d) = e$, then write $c'e = c$ and $d'e = d$ where $c', d' \in R$ and replace c/d with c'/d'. Then we have $c/d = c'e/d'e = c'/d'$ and by part 2 of this problem we have $\gcd(c', d') = 1$). Suppose c/d is integral over R, say

$$\frac{c^n}{d^n} + a_{n-1}\frac{c^{n-1}}{d^{n-1}} + a_{n-1}\frac{c^{n-2}}{d^{n-2}} + \cdots + a_0 = 0$$

for some $n \in \mathbb{N}$ and $a_0, \ldots, a_{n-1} \in R$. Clearing denominators and rearranging terms gives us

$$c^n = -d(a_{n-1}c^{n-1} + a_{n-2}dc^{n-2} + \cdots + a_0 d^{n-1})$$

In particular, we see that $d \mid c^n$. On the other hand, note that $\gcd(c, d) = 1$ implies $\gcd(c^2, d) = 1$ by part 3 of this problem. An easy induction argument also shows $\gcd(c^n, d) = 1$ too. Since $d \mid c^n$ and $d \mid d$, it follows that $d \mid 1$. In other words, d must be a unit in R, which implies $c/d \in R$. Thus R is integrally closed.

6. Suppose R is a Bezout domain. Then $\langle a, b\rangle = \langle d\rangle$ for some $d \in R$. We claim that d is a greatest common divisor of a and b. Indeed, we clearly have $a'd = a$ and $b'd = b$ for some $a', b' \in R$ since $\langle a, b\rangle = \langle d\rangle$. Thus $d \mid a$ and $d \mid b$, which means d is a divisor of a and b. Moreover, suppose there exists $d' \in R$ such that $d' \mid a$ and $d' \mid b$, say $a''d' = a$ and $b''d' = b$ for some $a'', b'' \in R$. Since $\langle a, b\rangle = \langle d\rangle$ there exists $x, y \in R$ such that $ax + by = d$. Then observe that

$$\begin{aligned}d &= ax + by\\ &= a''d'x + b''d'y\\ &= (a''x + b''y)d'\end{aligned}$$

implies $d' \mid d$ since R is a domain. It follows that $d = \gcd(a, b)$. Then $d = ax + by$ shows us that $\gcd(a, b)$ is a linear combination of a and b.

Conversely, let $d = \gcd(a, b)$ and suppose d is a linear combination of a and b, say $ax + by = d$ for some $x, y \in R$. Then this implies $\langle a, b\rangle \subseteq \langle d\rangle$. Furthermore, since d is a divisor of a and b, we have $a = a'd$ and $b = b'd$ for some $a', b' \in R$. This implies $\langle a, b\rangle \supseteq \langle d\rangle$. Thus we have $\langle a, b\rangle = \langle d\rangle$. It follows that R is a Bezout domain.

Problem 2

Exercise 2. Let R be a semiquasilocal domain and let I be an invertible ideal. Then I is principal.

Solution 2. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ be the maximal ideals of R. Since I is invertible, we have $II^{-1} = R$. In particular, for each $1 \leq i \leq n$ there exists $x_i \in I$ and $y_i \in I^{-1}$ such that $x_i y_i \notin \mathfrak{m}_i$. For each $i \neq j$, choose $z_{ji} \in \mathfrak{m}_j \backslash \mathfrak{m}_i$. Setting $z_i = \prod_{i \neq j} z_{ji}$, we see that $z_i \in \mathfrak{m}_j$ for all $i \neq j$ and $z_i \notin \mathfrak{m}_i$. Finally set

$$z = \sum_{i=1}^{n} z_i y_i.$$

Clearly $z \in I^{-1}$, and thus zI is an ideal in R. We claim that $zI = R$. To see this, assume for a contradiction that zI is contained in a maximal ideal. By relabeling indices if necessary, we may assume that $zI \subseteq \mathfrak{m}_1$. First note that

$$zx_1 = z_1 y_1 x_1 + \sum_{i=2}^{n} z_i y_i x_1.$$

By construction, we have $z_1 y_1 x_1 \notin \mathfrak{m}_1$ and $z_i y_i x_i \in \mathfrak{m}_1$ for all $i \neq 1$. Thus zx_1 is the sum of an element in $\mathfrak{m}_1$ with an element not in $\mathfrak{m}_1$. This is a contradiction since $zx_1 \in \mathfrak{m}_1$. It follows that $zI = R$, and hence $I = \langle z^{-1}\rangle$ is principal.

Problem 3

Notation: We write $\mathbb{N} = \{1, 2, \dots\}$, so $0 \notin \mathbb{N}$.

Exercise 3. Build a Noetherian domain of infinite Krull dimension.

Solution 3. Let K be a field and let $R = K[\{x_n \mid n \in \mathbb{N}\}]$. For each $k \in \mathbb{N}$, let $\mathfrak{p}_k = \langle x_{2^{k-1}}, x_{2^{k-1}+1}, \dots, x_{2^k-1} \rangle$. The sequence of ideals $(\mathfrak{p}_k)$ starts out as

$$\begin{aligned}
\mathfrak{p}_1 &= \langle x_1 \rangle \\
\mathfrak{p}_2 &= \langle x_2, x_3 \rangle \\
\mathfrak{p}_3 &= \langle x_4, x_5, x_6, x_7 \rangle \\
&\vdots
\end{aligned}$$

Note that each $\mathfrak{p}_k$ is a prime ideal. Indeed, suppose $f, g \in R$ such that $fg \in \mathfrak{p}_k$. Since f and g are polynomials, we must have $f, g \in R_N$ where $R_N = K[x_1, x_2, \dots, x_N]$ for some $N \in \mathbb{N}$. By choosing N large enough, we may assume that $2^k - 1 \leq N$ (in fact we already have this since $fg \in \mathfrak{p}_k$). Then $\mathfrak{p}_k \cap R_N$ is a prime ideal, so either $f \in \mathfrak{p}_k \cap R_N$ or $g \in \mathfrak{p}_k \cap R_N$. We already have $f, g \in R_N$, so either $f \in \mathfrak{p}_k$ or $g \in \mathfrak{p}_k$. It follows that each $\mathfrak{p}_k$ is prime.

Now let S be the multiplicative set

$$S = R \backslash \left(\bigcup_{k \in \mathbb{N}} \mathfrak{p}_k \right).$$

This set is multiplicatively closed since each $\mathfrak{p}_k$ is a prime ideal. We claim that R_S is a Noetherian ring of infinite dimension. We will show this in two steps.

Step 1: We prove a generalized prime avoidance for R. In particular, suppose I is an ideal of R such that $I \subseteq \bigcup_{k \in \mathbb{N}} \mathfrak{p}_k$. We claim that $I \subseteq \mathfrak{p}_k$ for some $k \in \mathbb{N}$. Indeed, assume for a contradiction that $I \not\subseteq \mathfrak{p}_k$ for any $k \in \mathbb{N}$. Clearly then $I \neq 0$. Choose a nonzero polynomial $f \in I$ and express it in terms of its monomials as

$$f = a_1 x^{\alpha_1} + \cdots + a_m x^{\alpha_m} \tag{1}$$

where $a_1, \dots, a_m \in K \backslash \{0\}$ and $\alpha_1, \dots, \alpha_m \in \mathcal{F}$ where $\alpha_i \neq \alpha_{i'}$ for all $1 \leq i < i' \leq m$.

Before proceeding with the proof, let us explain our notation in (1). Given a function $\alpha \colon \mathbb{N} \to \mathbb{Z}_{\geq 0}$, we define its **support**, denoted $\operatorname{supp} \alpha$, to be the set

$$\operatorname{supp} \alpha = \{m \in \mathbb{N} \mid \alpha(m) \neq 0\}.$$

We denote by $\mathcal{F}$ to be the set

$$\mathcal{F} = \{\alpha \colon \mathbb{N} \to \mathbb{Z}_{\geq 0} \mid \operatorname{supp} \alpha \text{ is finite}\}.$$

We also denote by $\mathcal{M}$ to be the set of all monomials in R. There is a bijection from $\mathcal{F}$ to $\mathcal{M}$ given by assigning $\alpha \in \mathcal{F}$ to the monomial

$$x^\alpha := \prod_{m \in \mathbb{N}} x_m^{\alpha(m)} = \prod_{m \in \operatorname{supp} \alpha} x_m^{\alpha(m)}.$$

For instance, suppose $\alpha \colon \mathbb{N} \to \mathbb{N}$ is defined by

$$\alpha(m) = \begin{cases} 3 & \text{if } m = 2 \\ 2 & \text{if } m = 6 \\ 4 & \text{if } m = 11 \\ 0 & \text{if } m \in \mathbb{N} \backslash \{2, 6, 11\} \end{cases}$$

Then $x^\alpha = x_3^3 x_6^2 x_{11}^4$ and $\operatorname{supp} \alpha = \{2, 6, 11\}$. We often pass back and forth between functions $\alpha \in \mathcal{F}$ and monimals $x^\alpha \in \mathcal{M}$. For example, given a monimal $x^\alpha \in \mathcal{M}$, we define its **support**, denoted $\operatorname{supp} x^\alpha$, to be $\operatorname{supp} x^\alpha = \operatorname{supp} \alpha$. Finally, in the monomial expansion of f given in (1), we refer to the $a_i x^{\alpha_i}$ as the **terms** of f, and we refer to the x^{α_i} as the **monomials** of f.

With our notation explained, we now proceed with the proof. For each $k \in \mathbb{N}$, we denote by C_k to be the set

$$C_k = \{2^{k-1}, 2^{k-1} + 1, \dots, 2^k - 1\}.$$

Observe that $f \in \mathfrak{p}_k$ if and only if $\operatorname{supp} x^{\alpha_i} \cap C_k \neq \emptyset$ for all monomials x^{α_i} of f. Or from the contrapositive point of view, we have $f \notin \mathfrak{p}_k$ if and only if $\operatorname{supp} x^{\alpha_i} \cap C_k = \emptyset$ for some monomial x^{α_i} of f. Since $\operatorname{supp} x^{\alpha_i}$ is finite for all monomials x^{α_i} of f, it follows that $\operatorname{supp} x^{\alpha_i} \cap C_k \neq \emptyset$ for only finitely many $k \in \mathbb{N}$. Since f has only finitely many monomials, it follows that there exists finitely many C_k's such that $\operatorname{supp} x^{\alpha_i} \cap C_k \neq \emptyset$ for some monomial x^{α_i} of f. Let $C_{k_1}, \dots, C_{k_s}$ be this finite collection, where $k_r \in \mathbb{N}$ for each $1 \leq r \leq s$ and $k_1 \neq \cdots \neq k_s$. So given $k \in \mathbb{N}$, if $k \neq k_r$ for any $1 \leq r \leq s$, then

$$\operatorname{supp} x^{\alpha_i} \cap C_k = \emptyset \tag{2}$$

for all monomials x^{α_i} of f. In particular, this implies $f \notin \mathfrak{p}_k$. Thus f is contained in at most finitely many of the $\mathfrak{p}_k$'s.

Now note that if $I \subseteq \bigcup_{r=1}^{s} \mathfrak{p}_{k_r}$, then by the usual prime avoidance argument, we would obtain $I \subseteq \mathfrak{p}_{k_r}$ for some $1 \leq r \leq s$, which would be a contradiction, thus we cannot have we $I \subseteq \bigcup_{r=1}^{s} \mathfrak{p}_{k_r}$. Hence there exists a $g \in I$ and an $l \in \mathbb{N}$ such that $l \neq k_r$ for any $1 \leq r \leq s$ and $g \in \mathfrak{p}_l \backslash \bigcup_{r=1}^{s} \mathfrak{p}_{k_r}$. Express g in terms of its monomials as

$$g = b_1 x^{\beta_1} + \cdots + b_n x^{\beta_n} \tag{3}$$

where $b_1, \dots, b_n \in K\backslash\{0\}$ and $\beta_1, \dots, \beta_n \in \mathcal{F}$ where $\beta_j \neq \beta_{j'}$ for all $1 \leq j < j' \leq m$. Since $g \in \mathfrak{p}_l$, we see that $\operatorname{supp} x^{\beta_j} \cap C_l \neq \emptyset$ for all monomials x^{β_j} of g. Since $\operatorname{supp} x^{\alpha_i} \cap C_l = \emptyset$ for all monomials x^{α_i} of f (take $k = l$ in (2)), it follows that $\alpha_i \neq \beta_j$ for all $1 \leq i \leq m$ and $1 \leq j \leq n$. It follows that $x^{\alpha_i} \neq x^{\beta_j}$ for all $1 \leq i \leq m$ and $1 \leq j \leq n$. Thus every monomial of $f + g$ has the form x^{α_i} for some $1 \leq i \leq m$ or x^{β_j} for some $1 \leq j \leq n$ (there is no combination between a monomial of f and a monomial in g in the monomial expansion of $f + g$). We claim that $f + g \notin \mathfrak{p}_k$ for any $k \in \mathbb{N}$. Indeed, let $k \in \mathbb{N}$. We consider two cases:

Case 1: Suppose $k = k_r$ for some $1 \leq r \leq s$. Then since $g \notin \mathfrak{p}_{k_r}$, there exists a monomial x^{β_j} of g such that $\operatorname{supp} x^{\beta_j} \cap C_{k_r} = \emptyset$. Since x^{β_j} is also a monomial of $f + g$, it follows that $f + g \notin \mathfrak{p}_{k_r}$.

Case 2: Suppose $k \neq k_r$ for any $1 \leq r \leq s$. Then $\operatorname{supp} x^{\alpha_i} \cap C_l = \emptyset$ for all monomials x^{α_i} of f (as in (2)), so in particular $\operatorname{supp} x^{\alpha_1} \cap C_l = \emptyset$. Since x^{α_1} is also a monomial of $f + g$, it follows that $f + g \notin \mathfrak{p}_l$.

Thus we have constructed a polynomial $f + g$ in I which does not belong to $\mathfrak{p}_k$ for any $k \in \mathbb{N}$. This is a contradiction since $I \subseteq \bigcup_{k \in \mathbb{N}} \mathfrak{p}_k$.

Step 2: We show that R_S satisfies the conditions of (0.1) (stated and proved in appendix) which implies R_S is Noetherian. We will also show that $\dim R_S = \infty$. First, let us describe the maximal ideals in R_S. Recall that the prime ideals in R_S correspond to the prime ideals in R which are disjoint from S. For any prime ideal $\mathfrak{p}$ in R, we have

$$\begin{aligned} \mathfrak{p} \cap S = \emptyset &\iff \mathfrak{p} \subseteq \bigcup_{k \in \mathbb{N}} \mathfrak{p}_k \\ &\iff \mathfrak{p} \subseteq \mathfrak{p}_k \text{ for some } k \in \mathbb{N}, \end{aligned}$$

where the last if and only if follows from step 1. In particular, we see that the maximal ideals of R_S are precisely the localizations of the $\mathfrak{p}_k$'s, that is, they are of the form $\mathfrak{p}_{k,S} = S^{-1}\mathfrak{p}_k$ for some $k \in \mathbb{N}$. By transitivity of localization, we have $(R_S)_{\mathfrak{p}_{k,S}} \cong R_{\mathfrak{p}_k}$, and $R_{\mathfrak{p}_k}$ is Noetherian since it is a localization of a Noetherian ring, namely

$$R_{\mathfrak{p}_k} \cong K(\{x_m \mid \{x_n \mid n \in \mathbb{N}\backslash C_k\})[\{x_n \mid n \in C_k\}]_{\langle \{x_n \mid n \in C_k\} \rangle}. \tag{4}$$

Thus the first condition in (0.1) is satisfied. As for the second condition, recall in step 1 we showed that every nonzero $f \in R$ is contained in only finitely many of the $\mathfrak{p}_k$'s, and so certainly every nonzero $f/s \in R_S$ is contained in only finitely many of the $\mathfrak{p}_{k,S}$'s. Thus both conditions of (0.1) hold, and hence R_S is Noetherian. Finally, note that the isomorphism (4) also shows us that

$$\begin{aligned} \dim R_S &\geq \dim R_{\mathfrak{p}_k} \\ &= 2^{k-1}. \end{aligned}$$

Taking $k \to \infty$ gives us $\dim R_S = \infty$.

Appendix

Problem 3

Lemma 0.1. *Let R be a commutative ring with identity such that*

1. *for each maximal ideal $\mathfrak{m}$ of R, the local ring $R_{\mathfrak{m}}$ is Noetherian;*
2. *for each $x \in R\backslash\{0\}$, the set of maximal ideals of R which contain x is finite.*

Then R is Noetherian.

Proof. Let I be a nonzero ideal in R. By the hypothesis of R, only finitely many maximal ideals can contain I, say $\mathfrak{m}_1, \dots, \mathfrak{m}_r$. Choose any nonzero x_0 in I and let $\mathfrak{m}_1, \dots, \mathfrak{m}_{r+s}$ be the maximal ideals which contain x_0. Since $\mathfrak{m}_{r+1}, \dots, \mathfrak{m}_{r+s}$ do not contain I, there exists $x_j \in I$ such that $x_j \notin \mathfrak{m}_{r+j}$ for each $1 \leq j \leq s$. Since for each $1 \leq i \leq r$ the localization $R_{\mathfrak{m}_i}$ is Noetherian, we see that $I_{\mathfrak{m}_i}$ is finitely-generated. Thus there exists $x_{s+1}, \dots, x_t$ in I whose images in $R_{\mathfrak{m}_i}$ generated $I_{\mathfrak{m}_i}$ for all $1 \leq i \leq r$.

We claim that $I_{\mathfrak{m}} = \langle x_0, \dots, x_t \rangle_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ of R. Indeed, if $\mathfrak{m} \neq \mathfrak{m}_k$ for any $1 \leq k \leq r+s$, then $x_0 \notin \mathfrak{m}$. Thus the image of x_0 is a unit in $I_{\mathfrak{m}}$ and $\langle x_0, \dots, x_t \rangle_{\mathfrak{m}}$, and hence

$$I_{\mathfrak{m}} = R_{\mathfrak{m}} = \langle x_0, \dots, x_t \rangle_{\mathfrak{m}}.$$

If $\mathfrak{m} = \mathfrak{m}_{r+j}$ for some $1 \leq j \leq s$, then $x_j \notin \mathfrak{m}$ and $I \cap (R \backslash \mathfrak{m}) \neq \emptyset$. Thus again we have

$$I_{\mathfrak{m}} = R_{\mathfrak{m}} = \langle x_0, \dots, x_t \rangle_{\mathfrak{m}}.$$

Finally, if $\mathfrak{m} = \mathfrak{m}_i$ for some $1 \leq i \leq r$, then by construction, we have $I_{\mathfrak{m}} = \langle x_0, \dots, x_t \rangle_{\mathfrak{m}}$. Thus our claim is proved. Since $I_{\mathfrak{m}} = \langle x_0, \dots, x_t \rangle_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ of R, it follows that $I = \langle x_0, \dots, x_t \rangle$. In particular, we see that I is finitely-generated, and hence R is Noetherian. $\square$