Name: Tuan Pham
ID: 4652218

Math 8201: General Algebra
Homework #3

20 | 25

5

① Let A be a commutative ring.

(a) We'll show that a formal series $f = \sum_{i=0}^{\infty} a_i X^i \in A[[X]]$ is invertible if and only if a_0 is invertible in A.

($\Rightarrow$) We'll prove the forward direction first because there seems to be more hypotheses than the backward direction. Let $f = (a_0, a_1, a_2, \dots) \in A[[X]]$. Suppose f is invertible and $g = (b_0, b_1, b_2, \dots) \in A[[X]]$ is the inverse of f. We know that $(1, 0, 0, \dots)$ is the unit element of $A[[X]]$. Thus $fg = (1, 0, \dots)$.

By the definition of product on $A[[X]]$, we have

$$fg = (a_0 b_0,\ a_1 b_0 + a_0 b_1,\ a_2 b_0 + a_1 b_1 + a_0 b_2, \dots)$$

Thus $fg = (1, 0, \dots)$ implies $a_0 b_0 = 1$. Therefore a_0 is invertible and b_0 is the inverse of a_0.

($\Leftarrow$) Let $f = (a_0, a_1, a_2, \dots) \in A[[X]]$ which have invertible a_0. We will find $g = (b_0, b_1, b_2, \dots) \in A[[X]]$ such that $fg = (1, 0, 0, \dots)$. This is equivalent to finding a sequence $b_0, b_1, b_2, \dots$ such that $a_0 b_0 = 1$

and $\sum_{i+j=n} a_i b_j = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 = 0$ for any $n \geq 1$. (*)

One common way to find a sequence is to find its entries inductively. Since a_0 is invertible, b_0 can be found: $b_0 = a_0^{-1}$. For $n=1$, (*) means $a_0 b_1 + a_1 b_0 = 0$. Then we can find $b_1 = -a_0^{-1}(a_1 b_0)$. Suppose that we have found $b_0, b_1, \ldots, b_k \in A$ such that

$$a_0 b_0 = 1, \quad \text{and} \qquad (**)$$

$$\sum_{i+j=k} a_i b_j = 0,$$

then we will find $b_{k+1} \in A$ such that $\sum_{i+j=k+1} a_i b_j = a_0 b_{k+1} + a_1 b_k + \cdots + a_{k+1} b_0 = 0$.

We choose $b_{k+1} = -a_0^{-1}(a_1 b_k + \cdots + a_{k+1} b_0)$. Therefore, we obtain a sequence $b_0, b_1, \ldots$ such that (**) holds for any $k \in \mathbb{N}$. Therefore $g = (b_0, b_1, b_2, \ldots)$ is the inverse of f.

(b) We'll show that a polynomial $f = (a_0, a_1, \ldots, a_n, 0, \ldots) \in A[x]$ is invertible if and only if a_0 is invertible and $a_1, \ldots, a_n$ are all nilpotent.

We'll show the backward direction first because if a_0 is invertible then f has an inverse $g = (b_0, b_1, b_2, \ldots) \in A[[x]]$. Then we'll try to use the fact that all $a_1, \ldots, a_n$ are nilpotent to show that only finitely many

b_i's can be nonzero. The forward direction seems to be harder.

($\Leftarrow$) Here we have a_0 is invertible and $a_1, \dots, a_n$ are all nilpotent. Then there exists $g = (b_0, b_1, b_2, \dots) \in A[[x]]$ such that $fg = (1, 0, 0, \dots)$.

By part (a), we know that the sequence $b_0, b_1, b_2, \dots$ has to satisfy

$$b_{k+1} = -a_0^{-1}(a_1 b_k + \cdots + a_{k+1} b_0), \text{ for every } k \geq 0.$$

Since $a_{n+1} = a_{n+2} = \cdots = 0$, we have

$$b_{k+1} = -a_0^{-1}(a_1 b_k + \cdots + a_n b_{k+1-n}), \text{ for every } k \geq n.$$

Using this fact, we'll show that b_{k+1} has an interesting representation in terms of $a_1, a_2, \dots, a_n$. Before doing so, we put

$$S_k = \{(i_1, i_2, \dots, i_k) : 1 \leq i_1, \dots, i_k \leq n\}$$

We will show by induction in $j \geq 1$ that for any $k \geq (j-1)n$, there exists $c^{(k)}_{i_1 \dots i_j} \in A$ for each $(i_1, \dots, i_j) \in S_j$ such that

$$b_{k+1} = \sum_{S_j} c^{(k)}_{i_1 \dots i_j} a_{i_1} a_{i_2} \cdots a_{i_j} \qquad (1)$$

For $j = 1$, we know that $b_{k+1} = -a_0^{-1}(a_1 b_k + \cdots + a_{k+1} b_0)$

$= c_1 a_1 + \cdots + c_n a_n$, which is obtained by deleting all zero a_i's and adding zero i's if a_i for some $i \in \{1, \dots, n\}$ a_i doesn't appear. Thus (1) is true for the base case $j = 1$.

4.

Suppose that (1) is true for $j \geq 1$. Let's show that it's also true for $j+1$. Let $k \geq jn$. We have

$$b_{k+1} = -a_0^{-1}\left(a_1 b_k + \cdots + a_n b_{k+1-n}\right)$$

Since $k+1-n \geq jn+1-n = (j-1)n+1$, we have

$$b_{k+1-n} = \sum_{f_j} \square\, a_{i_1} \cdots a_{i_j}$$

$$\cdots\cdots\cdots$$

$$b_k = \sum_{f_j} \square\, a_{i_1} \cdots a_{i_j}$$

thus $b_{k+1} = \sum_{f_{j+1}} \square\, a_{i_1} \cdots a_{i_j} a_{i_{j+1}}$. Here the squares $\square$ denote some elements in A that we are not interested in. Thus, (1) is also true for $j+1$.

Thus, we have $b_{k+1} = \sum_{f_j} \square\, a_{i_1} \cdots a_{i_j}$ for any $k \geq (j-1)n$.

Since $i_1, \ldots, i_j \in \{1, \ldots, n\}$, there exists an index, say i_1, that occurs at least $\left[\frac{j}{n}\right]$ times in the product $a_{i_1} \cdots a_{i_j}$.

Since $a_1, \ldots, a_n$ are nilpotents, there exists $\alpha_1, \ldots, \alpha_n \geq 0$ such that $a_1^{\alpha_1} = a_2^{\alpha_2} = \cdots = a_n^{\alpha_n} = 0$. We put $m = \max\{\alpha_1, \ldots, \alpha_n\}$. Then $a_1^m = \cdots = a_n^m = 0$.

We choose $j = mn$. Then $\left[\frac{j}{n}\right] = m$. Then each product $a_{i_1} \cdots a_{i_j}$ must be zero because it contains some $a_i^m = 0$. Thus $b_{k+1} = 0$ for all $k \geq (j-1)n$.

Thus $b_{k+1} = 0$ for all $k \geq (mn-1)n$. Therefore g is a polynomial and hence f is invertible in $A[X]$.

($\Longrightarrow$) Let $f = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots) \in A[X]$ be an invertible polynomial. We'll show that a_0 is invertible and $a_1, \dots, a_n$ are all nilpotents. First, since f is invertible as an element in $A[[X]]$, a_0 is invertible according to part (a). Let $g = (b_0, b_1, \dots, b_n, 0, 0 \dots) \in A[X]$ be the inverse of f in $A[x]$. In fact we have to write $b_0, \dots, b_m$ instead of $b_0, \dots, b_n$. However we can add finitely many "leading coefficient" which are zeros to make the two sequences $a_0, a_1, \dots, a_n$ and $b_0, b_1, \dots, b_m$ be of the same length. We have $fg = (1, 0, 0 \dots)$ and $a_0 b_0 = 1$.

By considering $a_0^{-1} f$ and $b_0^{-1} g$ instead of f and g, we can assume that $a_0 = b_0 = 1$. Then the condition $fg = (1, 0, 0, \dots)$ gives us

$$-b_{k+1} = a_1 b_k + a_2 b_{k-1} + \cdots + a_k b_1 + a_{k+1} \quad \forall k \geq 0 \qquad (*)$$

We will show that a_n is a nilpotent. After that we'll find a way to show inductively that $a_{n-1}, a_{n-2}, \dots, a_1$ are nilpotents. To do so, first we'll show by induction (in r) that $a_n^r b_{n+1-r} = 0$ for all $1 \leq r \leq n+1$. $(**)$

6

If we achieve this, then for $r = n+1$ we get $a_n^{n+1} = 0$, and thus a_n is a nilpotent. Because $a_m = b_m = 0$ for every $m > n$, the formula (*) gives us

$$a_{k+1-n} b_n + a_{k+2-n} b_{n-1} + \cdots + a_n b_{k+1-n} = 0 \quad \forall n \le k+1 \le 2n. \tag{***}$$

Choose $k+1 = 2n$, (***) gives $a_n b_n = 0$. Thus (**) is true for the base case $r = 1$. Suppose that we have $a_n^j b_{n+1-j} = 0$ $\forall 1 \le j \le r$ for some $1 \le r \le n$. We'll show that $a_n^{r+1} b_{n-r} = 0$. Choose $k+1 = 2n-r$, then (***) gives

$$0 = \sum_{j=1}^{r+1} a_{n-r+j-1} b_{n+1-j} = a_n b_{n-r} + \sum_{j=1}^{r} a_{n-r+j-1} b_{n+1-j}$$

Multiplying both sides by a_n^r, we get

$$0 = a_n^{r+1} b_{n-r} + \sum_{j=1}^{r} a_{n-r+j-1} a_n^{r-j} \underbrace{a_n^j b_{n+1-j}}_{0}$$

Thus $a_n^{r+1} b_{n-r} = 0$. Therefore (**) is true for all $1 \le r \le n+1$. Thus, a_n is a nilpotent in A.

Then we see that $a_n X^n$ is also nilpotent in $A[X]$. If we can show that $f - a_n X^n$ is also invertible, then the leading coefficient of

$$f(X) - a_n X^n = (a_0, a_1, \ldots, a_{n-1}, 0, \ldots)$$

is again a nilpotent. This means a_{n-2} is a nilpotent. Then we will show that $(a_0, a_1, \ldots, a_{n-2}, 0, 0 \ldots, 0)$ is invertible, which will again leads to a_{n-2} is a nilpotent. Therefore, it suffices for us to show that the difference between a unit an a nilpotent is also a unit.

In other words, we'll show that

"If $a \in U(R)$, where R is a commutative ring, and $b \in R$ is a nilpotent, then $a-b$ is also a unit."

In our problem, $R = A[X]$, $a = f$ and $b = a_n X^n$. Now we'll prove the lemma. Put $c = a^{-1}b$. Then $a - b = a(1-c)$. Thus it suffices to show that $1-c$ is a unit. Since b is a nilpotent and R is Commutative, c is also a nilpotent. Thus there exists $m \geq 1$ such that $c^m = 0$.

Thus,
$$(1-c)(1+c+\ldots+c^{m-1}) = 1 - c^m = 1$$

Therefore, $1-c$ is a unit.

5

② Let G be a finite abelian group whose order is not divisible by the square of any integer (the order is square-free). Then by Cor we can

8

write $\text{ord}(G) = n = p_1 \cdots p_k$ where $p_1, \ldots, p_k$ are distinct prime numbers. By Cauchy's theorem, there exists an element x_1 of order p_1, an element x_2 of order p_2, ..., and an element x_k of order p_k. Since all p_i's are distinct, $\langle x_i \rangle \cap \langle x_j \rangle = \{0\}$ if $i \neq j$. Thus $\langle x_1 \rangle \langle x_2 \rangle \cdots \langle x_k \rangle$ is a subgroup of G having order $p_1 p_2 \cdots p_k$. Thus $\langle x_1 \rangle \langle x_2 \rangle \cdots \langle x_k \rangle = G$.

Therefore, $G \simeq \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_k \rangle \simeq (\mathbb{Z}/p_1\mathbb{Z}) \times (\mathbb{Z}/p_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})$

$$\simeq \mathbb{Z}/(p_1 \cdots p_k)\mathbb{Z}$$

$$= \mathbb{Z}/n\mathbb{Z}$$

Since $(\mathbb{Z}/n\mathbb{Z}, +)$ is a cyclic group with the additive unit $\bar{1}$, G is also cyclic.

(a) First, we'll show that ~~there~~ $(G, +)$ can be equipped with a multiplicative structure to form a ring. Let $\phi : G \longrightarrow \mathbb{Z}/n\mathbb{Z}$ be a group-isomorphism. We see that $(\mathbb{Z}/n\mathbb{Z}, +)$ can be thought as a ring with the familiar multiplication $\bar{a}\bar{b} := \overline{ab}$. For each pair (x, y) in G, we define $xy := \phi^{-1}(\phi(x)\,\phi(y))$. We double-check that this is indeed a ring structure on G.

- $(xy)z = \phi^{-1}\left(\phi(xy)\,\phi(z)\right) = \phi^{-1}\left(\phi\left(\phi^{-1}(\phi(x)\,\phi(y))\right)\phi(z)\right)$

$= \phi^{-1}\left((\phi(x)\,\phi(y))\,\phi(z)\right)$

$= \phi^{-1}\left(\phi(x)\,(\phi(y)\,\phi(z))\right)$

$= \phi^{-1}\left(\phi(x)\,\phi(yz)\right) = x(yz).$

- Put $e = \phi^{-1}(\bar{1})$. Then

$xe = \phi^{-1}(\phi(x)\,\phi(e)) = \phi^{-1}(\phi(x)\,\bar{1}) = \phi^{-1}(\phi(x)) = x$

$ex = \phi^{-1}(\phi(e)\,\phi(x)) = \phi^{-1}(\bar{1}\,\phi(x)) = \phi^{-1}(\phi(x)) = x$

- We see that $xy = \phi^{-1}(\phi(x)\,\phi(y)) = \phi^{-1}(\phi(y)\,\phi(x))$ because $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring

$= yx.$

- $(x+y)z = \phi^{-1}(\phi(x+y)\,\phi(z)) = \phi^{-1}((\phi(x)+\phi(y))\,\phi(z))$

$= \phi^{-1}(\phi(x)\,\phi(z) + \phi(y)\,\phi(z))$

$= \phi^{-1}(\phi(x)\,\phi(z)) + \phi^{-1}(\phi(y)\,\phi(z))$

$= xz + yz$

By the commutativity, we get $x(y+z) = xy + xz$.

Therefore, G with the above multiplication is a commutative ring.

Next, we'll show that any other ring structure $(G, +, \circ)$ on G

must be ring-isomorphic to this one. Let $\dot{e}$ be the unit element of $(G,+,\cdot)$ and e' the unit element of $(G,+,\circ)$. We'll show that e is an additive generator of $(G,+)$. (Then symmetrically, e' is also an additive generator of $(G,+)$). Let m be the order of e in $(G,+)$. Then $m \neq 0$ because otherwise $e=0$ and G is the trivial group, which is a contradiction. Then for any $x \in G$,

$$mx = m(e\cdot x) = (m\cdot e)\cdot x = 0\cdot x = 0$$

Thus the order of x divides m. Since G is cyclic, there exists an element of order n, and any other element of G has order $\leq n$, $m \leq n$ and $n \mid m$. Therefore $m=n$ and thus e is an additive generator of $(G,+)$.

We define the following map $\Psi: (G,+,\cdot) \longrightarrow (G,+,\circ)$

$$re \longmapsto re'$$

for all $r \in \mathbb{Z}$. This definition automatically makes Ψ a group-isomorphism. To show that Ψ is a ring-isomorphism, we only need to show that Ψ respects the multiplicative structure.

We have $\psi(e) = e'$ and

$$\psi((r_1 e).(r_2 e)) = \psi(r_1 r_2 e) = r_1 r_2 e' = (r_1 e') \circ (r_2 e') = \psi(r_1 e) \circ \psi(r_2 e)$$

Therefore ψ is a ring-isomorphism. Thus, the ring structure that is compatible to the group structure on G is unique, up to an isomorphism.

(b) Let A denote the ring $(G, +, .)$ above. We'll show that the multiplicative group of invertible polynomials in $A[X]$ coincides with the multiplicative group A^* of invertible elements in A.

From part (a), we see that there is a ring-~~bo~~isomorphism $\phi: A \to \mathbb{Z}/n\mathbb{Z}$ where $n = p_1 p_2 \cdots p_k$. this isomorphism induces the corresponding ring-isomorphism from $A[[X]]$ to $(\mathbb{Z}/n\mathbb{Z})[[X]]$ and from $A[X]$ to $(\mathbb{Z}/n\mathbb{Z})[X]$. It will also induce a group isomorphism from $(A[X])^*$ to $(\mathbb{Z}/n\mathbb{Z})[X]^*$. Therefore, we should consider $\mathbb{Z}/n\mathbb{Z}$ instead of A. This consideration reduces the burden of abstractness in our mind.

Let $f = (a_0, a_1, \ldots, a_m, 0, 0, \ldots)$ be a polynomial over $\mathbb{Z}/n\mathbb{Z}$. Suppose that f is invertible, we'll show that $a_0 \in (\mathbb{Z}/n\mathbb{Z})^*$ and

$a_1 = \cdots = a_m = 0$. By Problem 1, part (b), we have $a_0 \in (\mathbb{Z}/n\mathbb{Z})^*$ and all $a_1, \ldots, a_m$ are nilpotents. It suffices to show that any nilpotent $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ must be $\bar{0}$. Suppose that $\bar{a}^r = \bar{0}$ for some $r \geq 1$. Then $n \mid a^r$, or $p_1 \cdots p_k \mid a^r$. Since each p_i is a prime number, we have $p_i \mid a$. Since ~~every~~ all p_i's are distinct, we have $p_1 \cdots p_k \mid a$, or equivalently $n \mid a$. Thus $\bar{a} = 0$.

Therefore every invertible polynomial over $\mathbb{Z}/n\mathbb{Z}$ must contain only the free coefficient $a_0 \in (\mathbb{Z}/n\mathbb{Z})^*$. Conversely, each $a_0 \in (\mathbb{Z}/n\mathbb{Z})^*$ is also a polynomial whose inverse is a_0^{-1}.

(c) First, we'll give an example (counterexample perhaps) to show that if the order of G is not square-free then there may be two non-isomorphic ring structure on G which are both compatible with the given group structure on G.

~~Put $(G,+) = (\mathbb{Z}/9\mathbb{Z}, +)$ be the finite abelian group of order $9 = 3^2$. Let $(G,+,\cdot)$ be the ring with usual multiplication: $\bar{a}\bar{b} = \overline{ab}$.~~

~~We define a binary operator (law of composition) as follow:~~

new

The easiest way to see that 2 rings are not isomorphic is to show that one is commutative, the other is not. Thus, we'll try to construct two kinds of multiplicative operators, one of which is commutative, the other is not. We know that two matrices have two ways of multiplication, one is the term by term multiplication, one is the usual as in linear algebra. We put

$$G = \left\{ \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} : \bar{a}, \bar{b}, \bar{c}, \bar{d} \in \mathbb{Z}/2\mathbb{Z} \right\}$$

Then G has the group structure by term-by-term addition, i.e.

$$\begin{pmatrix} \bar{a_1} & \bar{b_1} \\ \bar{c_1} & \bar{d_1} \end{pmatrix} + \begin{pmatrix} \bar{a_2} & \bar{b_2} \\ \bar{c_2} & \bar{d_2} \end{pmatrix} := \begin{pmatrix} \overline{a_1 + a_2} & \overline{b_1 + b_2} \\ \overline{c_1 + c_2} & \overline{d_1 + d_2} \end{pmatrix}$$

Moreover, G is an abelian group of order $2^4 = 16$. We define two following operators on G:

$$\begin{pmatrix} \bar{a_1} & \bar{b_1} \\ \bar{c_1} & \bar{d_1} \end{pmatrix} \cdot \begin{pmatrix} \bar{a_2} & \bar{b_2} \\ \bar{c_2} & \bar{d_2} \end{pmatrix} = \begin{pmatrix} \bar{a_1}\bar{a_2} + \bar{b_1}\bar{c_2} & \bar{a_1}\bar{b_2} + \bar{b_1}\bar{d_2} \\ \bar{c_1}\bar{a_2} + \bar{d_1}\bar{c_2} & \bar{c_1}\bar{d_2} + \bar{d_1}\bar{d_2} \end{pmatrix}$$

$$\begin{pmatrix} \bar{a_1} & \bar{b_1} \\ \bar{c_1} & \bar{d_1} \end{pmatrix} * \begin{pmatrix} \bar{a_2} & \bar{b_2} \\ \bar{c_2} & \bar{d_2} \end{pmatrix} = \begin{pmatrix} \bar{a_1}\bar{a_2} & \bar{b_1}\bar{b_2} \\ \bar{c_1}\bar{c_2} & \bar{d_1}\bar{d_2} \end{pmatrix}$$

14.

Then $(G,+,\cdot)$ is exactly the ring of 2×2 matrices over $\mathbb{Z}/2\mathbb{Z}$, and $(G,+,*)$ is isomorphic to the product ring $(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/2\mathbb{Z})$. The latter is commutative. We see that

$$\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{0} \end{pmatrix}\cdot\begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}, \text{ and}$$

$$\begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix}\cdot\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{0} \end{pmatrix}.$$

Thus $(G,+,\cdot)$ is not commutative. Therefore, these two rings are not isomorphic.

Next, we'll point out a counterexample to show that a commutative ring A whose order is not square-free may give rise to an invertible polynomial $f \in A[X]$ that is not in A^*.

Take $A = \mathbb{Z}/4\mathbb{Z}$ with usual addition and multiplication. Then A is a commutative ring of order 4. Put $f(X) = \bar{2}X + \bar{1}$. Then $f \notin A^*$ and $ff = (\bar{2}X+\bar{1})(\bar{2}X+\bar{1}) = \bar{1} + 2\bar{2}X + \bar{2}\bar{2}X^2 = 1$. Thus f is invertible.

(4) Let d be a square-free nonzero integer. $d \geq 1$ 5

First we'll show that if $m, n \in \mathbb{Z}$ satisfy $m + n\sqrt{d}$ then $m = n = 0$.

Proof. Suppose by contradiction that there exists a pair (m, n) in $(\mathbb{Z} \times \mathbb{Z}) \setminus \{0\}$ such that $m + n\sqrt{d} = 0$. Then there exists a pair (m_0, n_0) in $(\mathbb{Z} \times \mathbb{Z}) \setminus \{0\}$ satisfying $m_0 + n_0\sqrt{d} = 0$ with $|m_0| + |n_0|$ minimum.

We have $-m_0 = n_0\sqrt{d}$ and thus $m_0^2 = n_0^2 d$. Since d is square-free and $d > 1$, we can write d as a product of distinct prime numbers $d = p_1 \cdots p_k$. Since $d \mid m_0^2$, each $p_i \mid m_0^2$. Since p_i is a prime number, $p_i \mid m_0$. ~~Thus $p_i^2 \mid m_0^2$~~. Since $p_1^{a}, \ldots, p_k^{a}$ are relatively prime, $p_1^{a} \cdots p_k^{a} \mid m_0^{a}$. Thus $d^{a} \mid m_0$. We can put $m_0 = dk$ where $k \in \mathbb{Z} \setminus \{0\}$. Then the equation $m_0^2 = n_0^2 d$ becomes $k^2 d^2 = n_0^2 d$, or equivalently $n_0^2 = dk^2$. Thus (n_0, k) (or $(n_0, -k)$) is another pair in $(\mathbb{Z} \times \mathbb{Z}) \setminus \{0\}$ satisfying the equation $m + n\sqrt{d} = 0$. We see that

$$|n_0| + |\pm k| = |n_0| + |k| = |n_0| + \frac{|m_0|}{d} < |n_0| + |m_0|$$

This contradicts the choice of (m_0, n_0). Therefore, if m and n in $\mathbb{Z}$ satisfying $m + n\sqrt{d} = 0$ then $m = n = 0$.

#6

(i) We put $\mathbb{Z}[\sqrt{d}] = \{a+b\sqrt{d} \mid a,b \in \mathbb{Z}\}$

First we'll show that $\mathbb{Z}[\sqrt{d}]$ is an integral domain. Consider the following evaluation homomorphism coming from the fact that $\mathbb{Z}$ is a subring of $\mathbb{R}$.

$$ev : \mathbb{Z}[X] \longrightarrow \mathbb{R}$$
$$f \longmapsto f(\sqrt{d})$$

For any $a,b \in \mathbb{Z}$, we choose $f_{a,b}(X) = a+bX$ to see that $f_{a,b}(\sqrt{d}) = a+b\sqrt{d}$ and $ev(f_{a,b}) = a+b\sqrt{d}$. Therefore, $\mathbb{Z}[\sqrt{d}] \subset Im(ev)$. Conversely, For any $f = (a_0, a_1, \dots, a_n, 0, 0, \dots) \in \mathbb{Z}[X]$, we have

$$f(X) = \sum_{i=0}^{n} a_i X^i, \text{ and } f(\sqrt{d}) = \sum_{i=0}^{n} a_i (\sqrt{d})^i$$

Thus
$$f(\sqrt{d}) = \underbrace{\left(\sum_{\substack{0 \le i \le n \\ i \text{ even}}} a_i d^{i/2} \right)}_{\in \mathbb{Z}} + \sqrt{d} \underbrace{\left(\sum_{\substack{0 \le i \le n \\ i \text{ odd}}} a_i d^{(i-1)/2} \right)}_{\in \mathbb{Z}} \in \mathbb{Z}[\sqrt{d}]$$

Thus $Im(ev) \subset \mathbb{Z}[\sqrt{d}]$. Thus $\mathbb{Z}[\sqrt{d}] = Im(ev)$, which is a ring.

Now we'll show that $\mathbb{Z}[\sqrt{d}]$ has no zero-divisor. Suppose that there exists $x = a_1 + b_1\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ and $y = a_2 + b_2\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ such that $x \neq 0, y \neq 0$ and $xy = 0$. Then ...

$$0 = xy = (a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = (a_1a_2 + b_1b_2 d) + \sqrt{d}(a_1b_2 + a_2b_1)$$

Therefore we have

$$\begin{cases} a_1a_2 + b_1b_2 d = 0 \\ a_1b_2 + a_2b_1 = 0 \end{cases}$$

Regarding a_1 and b_1 as the unknowns, then we have a linear system of equations of a_1 and b_1. The determinant is

$$D = \begin{vmatrix} a_2 & db_2 \\ b_2 & a_2 \end{vmatrix} = a_2^2 - db_2^2$$

Since a_2 and b_2 are not zero at once, neither $a_2 - \sqrt{d}b_2 = 0$ nor $a_2 + \sqrt{d}b_2 = 0$. Thus, by the fact that $\mathbb{R}$ is an integral domain, $a_2^2 - db_2^2 = (a_2 - b_2\sqrt{d})(a_2 + b_2\sqrt{d}) \neq 0$. Thus $D \neq 0$. The system results in $a_1 = b_1 = 0$. This contradicts the assumption that $x \neq 0$. Therefore, $\mathbb{Z}[\sqrt{d}]$ is an integral domain.

(xx) Next, we'll show that $\mathbb{Z}[\sqrt{d}]$ is isomorphic to $\mathbb{Z}[X]/(X^2 - d)$. Since $\mathbb{Z}[\sqrt{d}] = \operatorname{Im} ev$, we have $\mathbb{Z}[\sqrt{d}] \simeq \mathbb{Z}[X]/\ker(ev)$. Thus what we need to show is $\ker(ev) = (X^2 - d)\mathbb{Z}[X]$.

For each $f \in (X^2 - d)\mathbb{Z}[X]$, we can write $f(X) = (X^2 - d)g(X)$

for some $g(X) \in \mathbb{Z}[X]$. Then $f(\sqrt{d}) = ((\sqrt{d})^2 - d)\, g(\sqrt{d}) = 0$. Thus $f \in \ker(ev)$. Thus $(X^2-d)\mathbb{Z}[X] \subset \ker(ev)$.

Next we'll show that $\ker(ev) \subset (X^2-d)\mathbb{Z}[X]$. Take $f \in \ker(ev)$. Then $f(\sqrt{d}) = 0$. We can write $f(X) = \sum_{i=0}^{n} a_i X^i$ where $a_i \in \mathbb{Z}$.

Then
$$f(\sqrt{d}) = \sum_{i=0}^{n} a_i (\sqrt{d})^i = \left(\sum_{\substack{0 \le i \le n \\ i \text{ even}}} a_i d^{i/2} \right) + \sqrt{d} \left(\sum_{\substack{0 \le i \le n \\ i \text{ odd}}} a_i d^{(i-1)/2} \right)$$

$$f(-\sqrt{d}) = \sum_{i=0}^{n} a_i (-\sqrt{d})^i = \left(\sum_{\substack{0 \le i \le n \\ i \text{ even}}} a_i d^{i/2} \right) - \sqrt{d} \left(\sum_{\substack{0 \le i \le n \\ i \text{ odd}}} a_i d^{(i-1)/2} \right)$$

Thus there are $m, n \in \mathbb{Z}$ such that $f(\sqrt{d}) = m + n\sqrt{d}$ and $f(-\sqrt{d}) = m - n\sqrt{d}$. Since $f(\sqrt{d}) = 0$, we get $m = n = 0$. Then $f(-\sqrt{d}) = 0$. Since f is a polynomial on $\mathbb{R}$, there exists $f_1 \in \mathbb{R}[X]$ such that $f(X) = (X - \sqrt{d}) f_1(X)$. Since $f(\sqrt{d}) = 0$, $f_1(-\sqrt{d}) = 0$. Thus there exist $g \in \mathbb{R}[X]$ such that $f_1(X) = (X + \sqrt{d})\, g(X)$. Thus we have $f(X) = (X^2 - d) g(X)$.

We have almost finished. What is left is to show that $g(X) \in \mathbb{Z}[X]$. We write $X^2 - d = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots)$ where $a_0 = -d$, $a_1 = 0$, $a_2 = 1$, and $a_k = 0$ for every $k > 2$. We write

$f(X) = (c_0, c_1, \dots, c_n, 0, 0, \dots)$, with $c_i \in \mathbb{Z}$,

$g(X) = (b_0, b_1, \dots, b_n, 0, 0, \dots)$, with $b_i \in \mathbb{Z}$.

By the fact that $(X^2 - d)\, g(X) = f(X)$, we'll show that each $b_i \in \mathbb{Z}$.

By the definition of product on $\mathbb{R}[X]$, we have

$$a_0 b_k + a_1 b_{k-1} + \dots + a_k b_0 = c_k \quad \text{for every } k \geq 0.$$

Since $a_j = 0$ for any $j \geq 3$, we get $a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} = c_k$ for every $k \geq 2$. Since $a_0 = -d$, $a_1 = 0$, $a_2 = 1$, we have $-d b_k + b_{k-2} = c_k$ for every $k \geq 2$. Thus,

$$b_{k-2} = c_k + d b_k, \quad \forall k \geq 2$$

Hence, to show that $b_0, b_1, \dots, b_n \in \mathbb{Z}$, it suffices to show that $b_n \in \mathbb{Z}$ and $b_{n-1} \in \mathbb{Z}$. The above formula gives us a way to prove by induction that $b_{n-2} \in \mathbb{Z}$, then $b_{n-3} \in \mathbb{Z}$, ..., then $b_0 \in \mathbb{Z}$. Take $k = n+1$, we get $b_{n-1} = c_{n+1} - d b_{n+1} = 0$. Take $k = n+2$, we get $b_n = c_{n+2} + d b_{n+2} = 0$.

Thus $b_{n-1} = b_n = 0 \in \mathbb{Z}$, whence the proof completes. 5

5 Let A and B be commutative rings, and we denote $N(A), N(B)$ the set of all nilpotents of A, B respectively.

20

(i) We will show that $N(A)$ is an ideal of A.

First, we show that $N(A)$ is a group. Since 0 is a nilpotent of A, $0 \in N(A)$. Let $x, y \in N(A)$. We can choose $m \geq 1$ such that $x^m = y^m = 0$. Then $m(x-y) = mx - my = 0$. Thus $x - y \in N(A)$.

Secondly, let $x \in A$ and $y \in N(A)$, we'll show that xy is also a nilpotent of A. There exists $m \geq 1$ such that $y^m = 0$. Then $(xy)^m = x^m y^m = x^m \cdot 0 = 0$. Thus $xy \in N(A)$. Therefore $N(A)$ is an ideal of A.

(ii) We'll show that $N(A \times B) = N(A) \times N(B)$.

- The "$\subset$" inclusion:

Let $(x, y) \in N(A \times B)$. Then there exists $m \geq 1$ such that $(x, y)^m = (0, 0)$.

By the definition of product on the product ring $A \times B$, we have

$$(x^m, y^m) = (x, y)^m = (0, 0)$$

Thus $x^m = y^m = 0$ and hence $x \in N(A)$, $y \in N(B)$.

- The "$\supset$" inclusion:

Let $x \in N(A)$ and $y \in N(B)$. We'll show that (x, y) is a nilpotent

of $A \times B$. there exists m and n such that $x^m = 0$ and $y^n = 0$.

Then $x^{m+n} = x^m x^n = 0$ and $y^{m+n} = y^m y^n = 0$. Thus $(x,y)^{m+n} = (0,0)$.

Thus (x,y) is a nilpotent of $A \times B$.

(iii) We will show that $N(A)$ is contained in every prime ideal of A.

Let $\underline{a}$ be a prime ideal of A. All what we know about $\underline{a}$ is that $A/\underline{a}$ is an integral domain. And this suggests an approach to show that $N(A) \subset \underline{a}$. That is to show that $N(A)$ is contained in the kernel of the canonical homomorphism $\phi : A \longrightarrow A/\underline{a}$.

In other words, we should show that $\phi(x) = 0$ for any nilpotent $x \in A$. Let x be such a nilpotent with $x^m = 0$ and $m \geq 1$. But $y = \phi(x) \in A/\underline{a}$. Then $y^m = \phi(x)^m = \phi(x^m) = \phi(0) = 0$. Thus $y\, y^{m-1} = 0$ implies either $y = 0$ or $y^{m-1} = 0$. Then if $y^{m-1} = 0$ we get $y = 0$ or $y^{m-2} = 0, \ldots$ In the end we always get $y = 0$.

In other words, an integral domain has only one nilpotent, that is 0. Thus $\phi(x) = 0$ and the proof completes.

The next step is to show that the intersection of all prime ideals

in A is contained in $N(A)$. We will show this later.

④ (cc) Take $x = a+b\sqrt{d}$ where $a, b \in \mathbb{Z}$. Let (x) be the principle ideal of x in $\mathbb{Z}[\sqrt{d}]$, i.e. $(x) = x\mathbb{Z}[\sqrt{d}]$. We will find a generator t for $(x) \cap \mathbb{Z}$, which is also an ideal in $\mathbb{Z}$ since $\mathbb{Z}$ is a subring of $\mathbb{Z}[\sqrt{d}]$.

- If $a = b = 0$ then $(x) = \{0\}$ and $(x) \cap \mathbb{Z} = \{0\}$. the generator of this trivial ideal is, perhaps by convention, $t = 0$.
- If a and b are not zero at once, we have

$$(x) = (a+b\sqrt{d})\mathbb{Z}[\sqrt{d}] = \{(a+b\sqrt{d})(u+v\sqrt{d}) : u, v \in \mathbb{Z}\}$$

$$= \{(au+bdv) + (av+bu)\sqrt{d} : u, v \in \mathbb{Z}\}$$

Thus $(x) \cap \mathbb{Z} = \{au+bdv : u, v \in \mathbb{Z} \text{ such that } av+bu = 0\}$.

Put $y = au+bdv$. We'll try to describe y through the following constraints

$$\begin{cases} au + bdv = y \\ bu + av = 0 \end{cases} \quad \text{and } u, v \in \mathbb{Z}.$$

The determinant is

$$D = \begin{vmatrix} a & bd \\ b & a \end{vmatrix} = a^2 - b^2 d.$$

Since a and b are not both zero, $D = (a-b\sqrt{d})(a+b\sqrt{d}) \neq 0$. Thus the above system of equations give unique solutions:

$$u = \frac{ay}{a^2 - db^2} \quad \text{and} \quad v = \frac{-by}{a^2 - db^2}$$

* If $a = 0$ then $u = 0$ and $v = \frac{-by}{-db^2} = \frac{y}{db}$. Thus all of the eligible y's are $y \in db\mathbb{Z}$. Thus,

$$(x) \cap \mathbb{Z} = db\mathbb{Z},$$

which implies that one generator for this ideal is $t = db$.

* If $b = 0$ then $v = 0$ and $u = \frac{ay}{a^2} = \frac{y}{a}$. Thus all of the eligible y's are $y \in a\mathbb{Z}$. Then $(x) \cap \mathbb{Z} = a\mathbb{Z}$. Thus one generator for this ideal is $t = a$.

* If $a \neq 0$ and $b \neq 0$, we put $\ell = \gcd(a, b)$ and write $a = a'\ell$ and $b = b'\ell$ where a' and b' are relatively prime. Then

$$u = \frac{ay}{a^2 - db^2} = \frac{a'y}{\ell(a'^2 - db'^2)}, \quad \text{and}$$

$$v = \frac{-by}{a^2 - dy^2} = \frac{-b'y}{\ell(a'^2 - db'^2)}.$$

Since $u, v \in \mathbb{Z}$, we should have $\ell \mid a'y$ and $\ell \mid b'y$. This is equivalent to $\ell \mid \gcd(a'y, b'y)$, which again is equivalent to $\ell \mid y$. We put $y' = \frac{y}{\ell}$.

Then $u = \dfrac{y'a'}{a'^2 - db'^2}$ and $v = \dfrac{-y'b'}{a'^2 - db'^2}$.

Since $u, v \in \mathbb{Z}$, we should have $(a'^2 \mp db'^2) \mid y'a'$ and $(a'^2 - db'^2) \mid y'b'$, which is equivalent to $(a'^2 - db'^2) \mid \gcd(y'a', y'b')$. This is again equivalent to $(a'^2 - db'^2) \mid y'$. Therefore, all eligible y's are such that $\ell(a'^2 - db'^2) \mid y$. In other words, $(x) \cap \mathbb{Z} = \ell(a'^2 - db'^2)\mathbb{Z}$. This implies one generator of the ideal is $t = \ell(a'^2 - db'^2)$.

Now we'll find a generator r of the ideal $A = \{m \in \mathbb{Z} \mid m\sqrt{d} \in (x)\}$ of $\mathbb{Z}$. The reason why A is an ideal of $\mathbb{Z}$ is that $A = \mathbb{Z} \cap \phi^{-1}((x))$ where ϕ is injective homomorphism $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}[\sqrt{d}]$, $\phi(m) = m\sqrt{d}$. We'll find a generator for A by repeating the preceding procedure.

We know that $(x) = \{(au + bdv) + (av + bu)\sqrt{d} : u, v \in \mathbb{Z}\}$. Thus,

$$A = \{m \in \mathbb{Z} \mid m\sqrt{d} = (au + bdv) + (av + bu)\sqrt{d} \text{ for some } u, v \in \mathbb{Z}\}$$

$$= \{m \in \mathbb{Z} \mid m = av + bu \text{ for some } u, v \in \mathbb{Z} \text{ such that } au + bdv = 0\}$$

We'll try to describe m through three constraints:

$$\begin{cases} bu + av = m \\ au + bdv = 0 \end{cases} \qquad \text{and } u, v \in \mathbb{Z}$$

The determinant is $D = \begin{vmatrix} b & a \\ a & bd \end{vmatrix} = b^2 d - a^2$.

* If $a = b = 0$ then $\phi(x) = 0$ and $\phi^{-1}(\phi(x)) = \phi^{-1}(0) = \ker\phi = \{0\}$ since ϕ is injective. Thus $A = A \cap \phi^{-1}(\phi(x)) = \{0\}$. Thus a generator of A is, perhaps by convention, $r = 0$.

* If a and b are not zero at once, then $D \neq 0$. The system of equations give unique solutions

$$u = \frac{-mbd}{a^2 - b^2 d} \qquad \text{and} \qquad v = \frac{ma}{a^2 - b^2 d}$$

* If $a = 0$ then $v = 0$ and $u = \dfrac{-mbd}{-b^2 d} = \dfrac{m}{b}$. All of the eligible m's are $m \in b\mathbb{Z}$. Thus $A = b\mathbb{Z}$ and one generator of its is $r = b$.

* If $b = 0$ then $u = 0$ and $v = \dfrac{m}{a}$. Then $A = a\mathbb{Z}$ and one generator of its is $r = a$.

* If $a \neq 0$ and $b \neq 0$, then we put $d = \gcd(a, bd)$ we then write

$a^* = la'$ and $b^* d = lc'$ where a' and c' are relatively prime.

Then,

$$u = \frac{-mbd}{a^2 - b^2 d} = \frac{-mlc'}{l^2 a'^2 - bdlc'} = \frac{-mc'}{la'^2 - bc'}, \text{ and}$$

$$v = \frac{ma}{a^2 - b^2 d} = \frac{mla'}{l^2 a'^2 - blc'} = \frac{ma'}{la'^2 - bc'}.$$

Since $u, v \in \mathbb{Z}$, we should have $(la'^2 - bc') \mid mc'$ and $(la'^2 - bc') \mid ma'$. This is equivalent to $(la'^2 - bc') \mid \gcd(mc', ma')$. This is again equivalent to $(la'^2 - bc') \mid m$. Thus,

$A = (la'^2 - bc')\mathbb{Z}$, and one generator of its is $r = la'^2 - bc'$.

Prob 3 from hw 0