HW 2

MINGFENG ZHAO

October 04, 2012

1. Show that $(\mathbf{Z}/m\mathbf{Z}) \otimes (\mathbf{Z}/n\mathbf{Z}) = 0$ if m, n are coprime.

Proof. Since m and n are coprime, then there exists some $s, t \in \mathbf{Z}$ such that

$$ms + nt = 1.$$

Now for any simple tensor $x \otimes y \in (\mathbf{Z}/m\mathbf{Z}) \otimes (\mathbf{Z}/n\mathbf{Z})$, we have

$$\begin{aligned} x \otimes y &= 1 \cdot (x \otimes y) \\ &= (ms + nt) \cdot (x \otimes y) \\ &= (ms) \cdot (x \otimes y) + (nt) \cdot (x \otimes y) \\ &= (msx) \otimes y + (ntx) \otimes y \\ &= (msx) \otimes y + x \otimes (tny) \\ &= 0 \otimes y + x \otimes 0 \\ &= 0 + 0 \\ &= 0. \end{aligned}$$

Since $(\mathbf{Z}/m\mathbf{Z}) \otimes (\mathbf{Z}/n\mathbf{Z})$ is generated by simple tensors, then we have

$$(\mathbf{Z}/m\mathbf{Z}) \otimes (\mathbf{Z}/n\mathbf{Z}) = 0.$$

□

2. Let A be a ring, $\mathfrak{a}$ an ideal, M an A-module. Show that $(A/\mathfrak{a}) \otimes_A M$ is isomorphic to $M/\mathfrak{a}M$.

Proof. Define $f : A/\mathfrak{a} \times M \to M/\mathfrak{a}M$ as: for all $x + \mathfrak{a} \in A/\mathfrak{a}$ and $m \in M$, we have

$$f(x + \mathfrak{a}, m) = xm + \mathfrak{a}M.$$

<u>Claim I</u>: f is well defined.

In fact, for all $x+\mathfrak{a}, y+\mathfrak{a} \in A/\mathfrak{a}$ and $m \in M$ such that $x+\mathfrak{a} = y+\mathfrak{a}$, then $x-y \in \mathfrak{a}$. Hence $xm = ym = (x-y)m \in \mathfrak{a}M$, in particular,

$$xm + \mathfrak{a}M = ym = \mathfrak{a}M.$$

That is, $f(x + \mathfrak{a}, m) = f(y + \mathfrak{a}, m)$. So f is well defined.

<u>Claim II</u>: f is an A-bilinear map.

In fact, for all $z \in A$, $x + \mathfrak{a}, y + \mathfrak{a} \in A/\mathfrak{a}$ and $m, n \in M$, then

$$\begin{aligned} f(z(x + \mathfrak{a}) + (y + \mathfrak{a}), m) &= f(zx + y + \mathfrak{a}, m) \\ &= (zx + y)m + \mathfrak{a}M \\ &= zxm + ym + \mathfrak{a}M \end{aligned}$$

$$
\begin{aligned}
&= (zxm+\mathfrak{a}M)+(ym+\mathfrak{a}M)\\
&= z(xm+\mathfrak{a}M)+(ym+\mathfrak{a}M)\\
&= zf(x+\mathfrak{a},m)+f(y+\mathfrak{a},m).\\
f(x+\mathfrak{a},zm+n) &= x(zm+n)+\mathfrak{a}M\\
&= zxm+xn+\mathfrak{a}M\\
&= (zxm+\mathfrak{a}M)+(xn+\mathfrak{a}M)\\
&= z(xm+\mathfrak{a}M)+(xn+\mathfrak{a}M)\\
&= zf(x+\mathfrak{a}M,m)+f(x+\mathfrak{a},n).
\end{aligned}
$$

Hence f is an A-bilinear map.

Since f is an A-bilinear map, by the universal property of tensor product, then there exists a unique A-module homomorphism $\varphi: A/\mathfrak{a}\otimes_A M\to M/\mathfrak{a}M$ such that for all $x\in A$ and $m\in M$, we have

$$\varphi((x+\mathfrak{a})\otimes m)=xm+\mathfrak{a}M.$$

Define another map $\psi: M/\mathfrak{a}M\to A/\mathfrak{a}\otimes_A M$ as: for all $m+\mathfrak{a}M$, we have

$$\psi(m+\mathfrak{a}M)=(1+\mathfrak{a})\otimes m.$$

<u>Claim III</u>: ψ is well defined.

In fact, for all $m,n\in M$ such that $m-n\in\mathfrak{a}M$, then there exists some $a\in\mathfrak{a}$ and $l\in M$ such that $m-n=al$. Hence

$$
\begin{aligned}
\psi(m+\mathfrak{a}M) &= (1+\mathfrak{a})\otimes m\\
&= (1+\mathfrak{a})\otimes(al+n)\\
&= (1+\mathfrak{a})\otimes(al)+(1+\mathfrak{a})\otimes n\\
&= [a(1+\mathfrak{a})]\otimes l+(1+\mathfrak{a})\otimes n\\
&= (a+\mathfrak{a})\otimes l+(1+\mathfrak{a})\otimes n\\
&= 0\otimes l+(1+\mathfrak{a})\otimes n\\
&= 0+(1+\mathfrak{a})\otimes n\\
&= (1+\mathfrak{a})\otimes n\\
&= \psi(n+\mathfrak{a}M).
\end{aligned}
$$

<u>Claim IV</u>: ψ is an A-module homomorphism.

In fact, for all $m,n\in M$ and $x\in A$, we have

$$
\begin{aligned}
\psi(x(m+\mathfrak{a}M)+n+\mathfrak{a}M) &= f(xm+n+\mathfrak{a}M)\\
&= (1+\mathfrak{a})\otimes(xm+n)\\
&= (1+\mathfrak{a})\otimes(xm)+(1+\mathfrak{a})\otimes n\\
&= x(1+\mathfrak{a})\otimes m+(1+\mathfrak{a})\otimes n\\
&= x\psi(m+\mathfrak{a}M)+\psi(n+\mathfrak{a}M).
\end{aligned}
$$

Hence ψ is an A-module homomorphism.

<u>Claim V</u>: $\psi\circ\varphi=Id$.

In fact for all simple tensor $(x+\mathfrak{a})\otimes m \in\in A/\mathfrak{a}\otimes_A M$, then

$$\begin{aligned}\psi\circ\varphi((x+\mathfrak{a})\otimes m) &= \psi(xm+\mathfrak{a}M)\\ &= (1+\mathfrak{a})\otimes(xm)\\ &= [x(1+\mathfrak{a})]\otimes m\\ &= (x+\mathfrak{a})\otimes m.\end{aligned}$$

Since $A/\mathfrak{a}\otimes_A M$ is generated by simple tensors, then $\psi\circ\varphi = Id$ on $A/\mathfrak{a}\otimes_A M$.

Claim VI: $\varphi\circ\psi = Id$.

For all $m+\mathfrak{a}M \in M/\mathfrak{a}M$, then

$$\begin{aligned}\varphi\circ\psi(m+\mathfrak{a}M) &= \varphi((1+\mathfrak{a})\otimes m)\\ &= 1m+\mathfrak{a}M\\ &= m+\mathfrak{a}M.\end{aligned}$$

Hence $\varphi\circ\psi = Id$ on $M/\mathfrak{a}M$.

In summary, we know that φ and ψ are A-module isomorphisms. Hence we know that $(A/\mathfrak{a})\otimes_A M$ is isomorphic to $M/\mathfrak{a}M$.

□

3. Let A be a local ring, M and N finitely generated A-modules. Prove that if $M\otimes_A N = 0$, then $M = 0$ or $N = 0$.

Proof. Since A is a local ring, then A has a unique maximal ideal $\mathfrak{m}$ in A. Since $\mathfrak{m}$ is the unique maximal ideal in A, then the Jacobson radical J of A is equal to $\mathfrak{m}$ and $k = A/\mathfrak{m}$ is a field.

For any A-module L, let $L_k = k\otimes_A L$. By the result of the Problem 2, then

$$L_k = k\otimes_A L = A/\mathfrak{m}\otimes_A L \cong L/\mathfrak{m}L.$$

Then L_k is a k-vector space. Since $M\otimes_A N = 0$, then $(M\otimes_A N)_k = 0$. On the other hand, since $k\otimes_k k = k$, then we know that

$$\begin{aligned}(M\otimes_A N)_k &= k\otimes_A(M\otimes_A N)\\ &= k\otimes_A M\otimes_A N\\ &= M\otimes_A k\otimes_A N\\ &= M\otimes_A(k\otimes_k k)\otimes_A N\\ &= (M\otimes_A k)\otimes_k(k\otimes_A N)\\ &= M_k\otimes_k N_k.\end{aligned}$$

Hence $M_k\otimes_k N_k = 0$. Since $M_k\otimes_k N_k$ is a k-vector space of dimension $\dim M_k\cdot\dim N_k$. Hence we must have $M_k = 0$ or $N_k = 0$. Without loss of generality, we assume $M_k = 0 = k\otimes_A M \cong M/\mathfrak{m}M$. Hence we get

$$M = \mathfrak{m}M.$$

Since $J = \mathfrak{m}$ and M, N are finitely generated A-modules, by the Nakayama's Lemma, we know that $M = 0$.

□

4. Let $M_i (i\in I)$ be any family of A-modules, and let M be their direct sum. Prove that M is flat $\Longleftrightarrow$ each M_i is flat.

Proof. ($\Longrightarrow$) Assume $M = \bigoplus_{i\in I} M_i$ is flat. For all $i \in I$, define $\pi_i : M \to M_i$ as the i-th projection, that is, for all $(m_j)_{j\in I} \in M$, we have

$$\pi((m_j)_{j\in I}) = m_i.$$

Let $e_i : M_i \to M$ as the i-th embedding, that is, for all $m_i \in M_i$, let $m_j = m_i$ if $i = j$ and $m_j = 0$ if $i \neq j$, then we have

$$e_i(m_i) = (m_j)_{j\in I}.$$

Now for any A-modules N and N' with any injective A-module homomorphism $f : N \to N'$. Since M is flat, then

$$f \otimes 1_M : N \otimes_A M \to N' \otimes_A M \quad \text{is injective.}$$

Let $\overline{f} : N \to f(N) \subset N'$, then $\overline{f}$ is bijective. Since M is flat, then

$$\overline{f} \otimes 1_M : N \otimes_A M \to f(N) \otimes_A M \quad \text{is injective.}$$

Since

$$N \otimes_A M = N \otimes_A (\bigoplus_{i\in I} M_i) = \bigoplus_{i\in I}(N \otimes_A M_i), \quad \text{and} \quad N' \otimes_A M = N' \otimes_A (\bigoplus_{i\in I} M_i) = \bigoplus_{i\in I}(N' \otimes_A M_i)$$

Then

$$1_N \otimes e_i : N \otimes_A M_i \to N \otimes_A M \quad \text{is injective.}$$

So we get

$$(f \otimes 1_M) \circ (1_N \otimes e_i) : N \otimes_A M_i \to N' \otimes_A M \quad \text{is injective.}$$

Now for $f \otimes 1_{M_i} : N \otimes_A M_i \to N' \otimes_A M_i$, we want to show that $f \otimes 1_{M_i}$ is injective, since $f \otimes 1_{M_i}(N \otimes_A M_i) \subset f(N) \otimes_A M_i$, then it suffices to show $\overline{f} \otimes 1_{M_i} : N \otimes_A M_i \to f(N') \otimes_A M_i$ is injective. Since $1_{M_i} = \pi_i \circ 1_M \circ e_i$, then

$$\overline{f} \otimes 1_{M_i} = (1_{f(N)} \otimes \pi_i) \circ (\overline{f} \otimes 1_M) \circ (1_N \otimes e_i).$$

Hence $\overline{f} \otimes 1_{M_i}$ is injective. So we know that $f \otimes 1_{M_i} : N \otimes_A M_i \to N' \otimes_A M_i$ is injective. Therefore, we know that M_i is flat for all $i \in I$.

($\Longleftarrow$) Assume that for all $i \in I$, M_i is flat. Now for any A-modules N and N' with any injective A-module homomorphism $f : N \to N'$. Since M_i is flat, then

$$f \otimes 1_{M_i} : N \otimes_A M_i \to N' \otimes_A M_i \quad \text{is injective.}$$

Now consider $f \otimes 1_M : N \otimes_A M \to N' \otimes_A M$, for any $\sum_{\text{finite}} n_j \otimes (m_i^j)_{i\in I} \in \ker f \otimes 1_M$, that is,

$$f \otimes 1_M \left(\sum_{\text{finite}} n_j \otimes (m_i^j)_{i\in I} \right) = 0$$

Then

$$\begin{aligned}
0 &= f \otimes 1_M \left(\sum_{\text{finite}} n_j \otimes (m_i^j)_{i\in I} \right) \\
&= \sum_{\text{finite}} f(n_j) \otimes (m_i^j)_{i\in I} \\
&= \left(\sum_{\text{finite}} f(n_j) \otimes m_i^j \right)_{i\in I} \\
&= \left((f \otimes 1_{M_i}) \left(\sum_{\text{finite}} n_j \otimes m_i^j \right) \right)_{i\in I}
\end{aligned}$$

Then we know that

$$(f \otimes 1_{M_i}) \left(\sum_{\text{finite}} n_j \otimes m_i^j \right) = 0, \quad \forall i \in I.$$

Since $f \otimes 1_{M_i}$ is injective, then

$$\sum_{\text{finite}} n_j \otimes m_i^j = 0, \quad \forall i \in I.$$

Which implies that

$$\sum_{\text{finite}} n_j \otimes (m_i^j)_{i \in I} = 0.$$

Hence $f \otimes 1_M$ is injective. Therefore, M is flat.

□

5. Let $A[x]$ be the ring of polynomials in one indeterminate over a ring A. Prove that $A[x]$ is a flat A-algebra.

Proof. We know that $A[x]$ is a ring such that A is a subring of $A[x]$, which implies that $A[x]$ is an A-module. So for all $i \geq 0$, Ax^i is an A-module generated by x^i in $A[x]$.
Claim I: $Ax^i \cong A$ as A-modules.

Define $\phi : A \to Ax^i$ as $\phi(a) = ax^i$, it is easy to see that ϕ is a bijective A-module homomorphism (Since $ax^i = 0$ iff $a = 0$), so $Ax^i \cong A$ as A-modules. Since A is a flat A-module, then Ax^i is also flat as A-module for all $i \geq 0$. On the other hand, since

$$A[x] = \bigoplus_{i=0}^{\infty} Ax^i, \quad \text{as } A\text{-modules}.$$

By the result of the Problem 4, we know that $A[x]$ is a flat A-module. Let $i : A \to A[x]$ be the embedding of rings, that is, $i(a) = a$ for all $a \in A$, then $A[x]$ is an A-algebra. Hence we know that $A[x]$ is a flat A-algebra.

□

6. For any A-module M, let $M[x]$ denote the set of all polynomials in x with coefficients in M, that is to say expressions of the form

$$m_0 + m_1 x + \cdots + m_r x^r, \quad m_i \in M.$$

Defining the product of an element of $A[x]$ and an element of $M[x]$ in the obvious way, show that $M[x]$ is an $A[x]$-module. Show that $M[x] \cong A[x] \otimes_A M$.

Proof. For any $\sum_{i=0}^{t} a_i x^i \in A[x]$ and $\sum_{i=0}^{r} m_i x^i \in M[x]$, let

$$\left(\sum_{i=0}^{t} a_i x^i \right) \cdot \left(\sum_{i=0}^{r} m_i x^i \right) = \sum_{i=0}^{t+r} \left(\sum_{j_1 + j_2 = i} a_{j_1} m_{j_2} \right) x^i.$$

Claim I: $M[x]$ is an $A[x]$-module

It is easy to see that $M[x]$ is an additive group, and the above scalar multiplication by $A[x]$ is well defined. For all $\sum_{i=0}^{r} m_i x^i \in M[x]$, we have

$$1 \cdot \left(\sum_{i=0}^{r} m_i x^i \right) = \sum_{i=0}^{r} m_i x^i.$$

It is easy to see that the distribution laws hold for this scalar multiplication. Now we only need to check the associativity law. In fact, for any $\sum_{i=0}^{t} a_i x^i, \sum_{i=0}^{s} b_i x^i \in A[x]$ and any $\sum_{i=0}^{r} m_i x^i \in M[x]$, we know that

$$\begin{aligned}
\left[\left(\sum_{i=0}^{t} a_i x^i\right)\left(\sum_{i=0}^{s} b_i x^i\right)\right]\cdot\left(\sum_{i=0}^{r} m_i x^i\right) &= \left[\sum_{i=0}^{t+s}\left(\sum_{j_1+j_2=i} a_{j_1}b_{j_2}\right)x^i\right]\cdot\left(\sum_{i=0}^{r} m_i x^i\right) \\
&= \sum_{i=0}^{t+s+r}\left(\sum_{j_4+j_3=i}\left(\sum_{j_1+j_2=j_4} a_{j_1}b_{j_2}\right)m_{j_3}\right)x^i \\
&= \sum_{i=0}^{t+s+r}\left(\sum_{j_1+j_2+j_3=i} a_{j_1}b_{j_2}m_{j_3}\right)x^i \\
\left(\sum_{i=0}^{s} b_i x^i\right)\cdot\left(\sum_{i=0}^{r} m_i x^i\right) &= \sum_{i=0}^{s+r}\left(\sum_{j_2+j_3=i} b_{j_2}m_{j_3}\right)x^i \\
\left(\sum_{i=0}^{t} a_i x^i\right)\cdot\left[\left(\sum_{i=0}^{s} b_i x^i\right)\cdot\left(\sum_{i=0}^{r} m_i x^i\right)\right] &= \left(\sum_{i=0}^{t} a_i x^i\right)\cdot\left[\sum_{i=0}^{s+r}\left(\sum_{j_2+j_3=i} b_{j_2}m_{j_3}\right)x^i\right] \\
&= \sum_{i=0}^{t+s+r}\left(\sum_{j_1+j_4=i} a_{j_1}\left(\sum_{j_2+j_3=j_3} b_{j_2}m_{j_3}\right)\right)x^i \\
&= \sum_{i=0}^{t+s+r}\left(\sum_{j_1+j_2+j_3=i} a_{j_1}b_{j_2}m_{j_3}\right)x^i \\
&= \left[\left(\sum_{i=0}^{t} a_i x^i\right)\left(\sum_{i=0}^{s} b_i x^i\right)\right]\cdot\left(\sum_{i=0}^{r} m_i x^i\right)
\end{aligned}$$

In summary, we know that $M[x]$ is an $A[x]$-module.

<u>Claim II</u>: $M[x] \cong A[x] \otimes_A M$ as $A[x]$-modules.

Define the map $\phi : A[x] \times M \to M[x]$ as: for all $\sum_{i=0}^{r} a_i x^i \in A[x]$ and all $m \in M$, we have

$$\varphi\left(\sum_{i=0}^{r} a_i x^i, m\right) = \sum_{i=0}^{r} (a_i m) x^i$$

It is easy to see that ϕ is well defined an A-bilinear map, by the universal property of tensor product, then there exists a unique A-module homomorphism $\Phi : A[x] \otimes_A M \to M[x]$ such that for all $\sum_{i=0}^{t} a_i x^i \in A[x]$ and all $m \in M$, we have

$$\Phi\left(\left(\sum_{i=0}^{t} a_i x^i\right) \otimes m\right) = \sum_{i=0}^{t} (a_i m) x^i$$

Now we need to check that Φ is an $A[x]$-module homomorphism, it suffices to check the $A[x]$-linearity for the simple tensors. In fact, for all $\sum_{i=0}^{t} a_i x^i, \sum_{i=0}^{s} b_i x^i \in A[x]$ and $m \in M$, we have

$$\Phi\left(\left(\sum_{i=0}^{s} b_i x^i\right)\left(\left(\sum_{i=0}^{t} a_i x^i\right) \otimes m\right)\right) = \Phi\left(\left(\sum_{i=0}^{s} b_i x^i\right)\left(\left(\sum_{i=0}^{t} a_i x^i\right)\right) \otimes m\right)$$

$$
\begin{aligned}
&= \Phi\left(\left(\sum_{i=0}^{t+s}\left(\sum_{j_1+j_2=i} b_{j_1}a_{j_2}\right)x^i\right)\otimes m\right)\\
&= \sum_{i=0}^{t+s}\left(\sum_{j_1+j_2=i} b_{j_1}a_{j_2}\right)mx^i\\
&= \left(\sum_{i=0}^{t+s}\left(\sum_{j_1+j_2=i} b_{j_1}a_{j_2}\right)x^i\right)\cdot m\\
&= \left[\left(\sum_{i=0}^{s} b_i x^i\right)\left(\sum_{i=0}^{t} a_i x^i\right)\right]\cdot m\\
&= \left(\sum_{i=0}^{s} b_i x^i\right)\cdot\left[\left(\sum_{i=0}^{t} a_i x^i\right)\cdot m\right]\\
&= \left(\sum_{i=0}^{s} b_i x^i\right)\cdot\Phi\left(\left(\sum_{i=0}^{t} a_i x^i\right)\otimes m\right)
\end{aligned}
$$

Also the additivity follows from A-module homomorphism. Hence Φ is an $A[x]$-module homomorphism. Define $\Psi : M[x] \to A[x]\otimes_A M$ as: for all $\sum_{i=0}^{r} m_i x^i \in M[x]$, we have

$$
\Psi\left(\sum_{i=0}^{r} m_i x^i\right) = \sum_{i=0}^{r} x^i \otimes m_i
$$

It is easy to see that Ψ is a well defined additive group homomorphism, now we need to check $A[x]$-linearity. For any $\sum_{i=0}^{t} a_i x^i \in A[x]$ and $\sum_{i=0}^{r} m_i x^i \in M[x]$, then

$$
\begin{aligned}
\Psi\left(\left(\sum_{i=0}^{t} a_i x^i\right)\cdot\left(\sum_{i=0}^{r} m_i x^i\right)\right) &= \Psi\left(\sum_{i=0}^{t+r}\left(\sum_{j_1+j_2=i} a_{j_1}m_{j_2}\right)x^i\right)\\
&= \sum_{i=0}^{t+r} x^i\otimes\left(\sum_{j_1+j_2=i} a_{j_1}m_{j_2}\right)\\
&= \sum_{i=0}^{t+r}\sum_{j_1+j_2=i} x^i\otimes(a_{j_1}m_{j_2})\\
&= \sum_{i=0}^{t+r}\sum_{j_1+j_2=i} (a_{j_1}x^i)\otimes m_{j_2}\\
&= \sum_{i=0}^{t+r}\sum_{j_1+j_2=i} ((a_{j_1}x^{j_1})x^{j_2})\otimes m_{j_2}\\
&= \sum_{i=0}^{t+r}\sum_{j_1+j_2=i} (a_{j_1}x^{j_1})\cdot(x^{j_2}\otimes m_{j_2})\\
&= \sum_{i=0}^{t+r}\sum_{j_1+j_2=i} (a_{j_1}x^{j_1})\cdot\Psi((m_{j_2}x^{j_2})
\end{aligned}
$$

$$= \left(\sum_{i=0}^{t} a_i x^i\right) \cdot \Psi\left(\sum_{i=0}^{r} m_i x^i\right)$$

Hence Ψ is $A[x]$-module homomorphism. Now for any $\sum_{i=0}^{r} m_i x^i \in M[x]$, then

$$\begin{aligned} \Phi \circ \Psi\left(\sum_{i=0}^{r} m_i x^i\right) &= \Phi\left(\sum_{i=0}^{r} x^i \otimes m_i\right) \\ &= \sum_{i=0}^{r} \Phi(x^i \otimes m_i) \\ &= \sum_{i=0}^{r} m_i x^i. \end{aligned}$$

That is, $\Phi \circ \Psi = Id$. Now for any $\sum_{i=0}^{r} a_i x^i \in A[x]$ and all $m \in M$, we have

$$\begin{aligned} \Psi \circ \Phi\left(\left(\sum_{i=0}^{r} a_i x^i\right) \otimes m\right) &= \Psi\left(\sum_{i=0}^{r} (a_i m) x^i\right) \\ &= \sum_{i=0}^{r} x^i \otimes (a_i m) \\ &= \sum_{i=0}^{r} (a_i x^i) \otimes m \\ &= \left(\sum_{i=0}^{r} (a_i x^i)\right) \otimes m. \end{aligned}$$

Which implies that $\Psi \circ \Phi = Id$. Therefore, we know that Φ and Ψ are $A[x]$-module isomorphisms, in particular, $M[x] \cong A[x] \otimes_A M$ as $A[x]$-modules.

□

15. Let A be a ring and let X be the set of all prime ideals of A. For each subset E of A, let $V(E)$ denote the set of all prime ideals of A which contain E. Prove that

a. If $\mathfrak{a}$ is the ideal generated by E, then $V(E) = V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$.
b. $V(0) = X$, $V(1) = \emptyset$.
c. If $(E_i)_{i \in I}$ is any family of subsets of A, then

$$V\left(\bigcup_{i \in I} E_i\right) = \bigcap_{i \in I} V(E_i).$$

d. $V(\mathfrak{a} \bigcap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \bigcup V(\mathfrak{b})$ for any ideals $\mathfrak{a}, \mathfrak{b}$ of A.

Proof. a. Since $E \subset \mathfrak{a} \subset \sqrt{\mathfrak{a}}$, then

$$V(\sqrt{\mathfrak{a}}) \subset V(\mathfrak{a}) \subset V(E).$$

Now for any prime ideal $\mathfrak{p}$ of A such that $E \subset \mathfrak{p}$, by the definition of $\mathfrak{a}$, then $\mathfrak{a} \subset \mathfrak{p}$, that is, $\mathfrak{p} \in V(\mathfrak{a})$. Also since $\mathfrak{a} \subset \mathfrak{p}$, then $\sqrt{\mathfrak{a}} \subset \sqrt{\mathfrak{p}}$. Since $\mathfrak{p}$ is prime, then $\sqrt{\mathfrak{p}} = \mathfrak{p}$. Hence $\sqrt{\mathfrak{a}} \subset \mathfrak{p}$, that is, $\mathfrak{p} \in V(\sqrt{\mathfrak{p}})$.

Therefore, we know that

$$V(\sqrt{\mathfrak{a}} = V(\mathfrak{a}) = V(E).$$

b. For any prime ideal $\mathfrak{p}$ of A, we know that $0 \in \mathfrak{p}$, then $\mathfrak{p} \in V(0)$. Hence

$$V(0) = X.$$

For $V(1)$, we must have $V(1) = \emptyset$, otherwise, there exists some prime ideal $\mathfrak{p}$ of A such that $1 \in \mathfrak{p}$, which implies that $\mathfrak{p} = A$, contradiction. Hence

$$V(1) = \emptyset.$$

c. Since for $i \in I$, we have $E_i \subset \bigcup_{i \in I} E_i$, then

$$V\left(\bigcup_{i \in I} E_i\right) \subset V(E_i), \quad \forall i \in I.$$

Hence

$$V\left(\bigcup_{i \in I} E_i\right) \subset \bigcap_{i \in I} V(E_i).$$

On the other hand, for all $\mathfrak{p} \in \bigcap_{i \in I} V(E_i)$, then

$$\mathfrak{p} \in V(E_i), \quad \forall i \in I.$$

That is,

$$E_i \subset \mathfrak{p}, \quad \forall i \in I.$$

Hence

$$\bigcup_{i \in I} E_i \subset \mathfrak{p}.$$

That is, $\mathfrak{p} \in V\left(\bigcup_{i \in I} E_i\right)$. Therefore, we know that

$$V\left(\bigcup_{i \in I} E_i\right) = \bigcap_{i \in I} V(E_i).$$

d. For any ideals $\mathfrak{a}, \mathfrak{b}$ of A, then

$$\mathfrak{ab} \subset \mathfrak{a} \bigcap \mathfrak{b} \subset \mathfrak{a}, \quad \text{and} \quad \mathfrak{ab} \subset \mathfrak{a} \bigcap \mathfrak{b} \subset \mathfrak{b}.$$

So we have

$$V(\mathfrak{a}) \subset V(\mathfrak{a} \bigcap \mathfrak{b}) \subset V(\mathfrak{ab}), \quad \text{and} \quad V(\mathfrak{a}) \subset V(\mathfrak{a} \bigcap \mathfrak{b}) \subset V(\mathfrak{ab}).$$

Hence

$$V(\mathfrak{a}) \bigcup V(\mathfrak{b}) \subset V(\mathfrak{a} \bigcap \mathfrak{b}) \subset V(\mathfrak{ab})$$

Now for any $\mathfrak{p} \in V(\mathfrak{ab})$, then $\mathfrak{ab} \subset \mathfrak{p}$ and $\mathfrak{p}$ is prime ideal, which implies that $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$, that is, $\mathfrak{p} \in V(\mathfrak{a}) \bigcup V(\mathfrak{b})$. Therefore, we get

$$V(\mathfrak{a}) \bigcup V(\mathfrak{b}) = V(\mathfrak{a} \bigcap \mathfrak{b}) = V(\mathfrak{ab})$$

□

16. Draw pictures of Spec ($\mathbf{Z}$), Spec ($\mathbf{R}$), Spec ($\mathbf{C}[x]$), Spec ($\mathbf{R}[x]$) and Spec ($\mathbf{Z}[x]$).

Proof. a. For $\mathbf{Z}$ which is a PID, the ideal $\mathfrak{p}$ of $\mathbf{Z}$ is prime if and only if $\mathfrak{p} = 0$ or $\mathfrak{p} = p\mathbf{Z}$ for some prime number p in $\mathbf{Z}$, that is,

$$\text{Spec } \mathbf{Z} = \{p\mathbf{Z} : p \text{ is a prime number in } \mathbf{Z} \text{ or } p = 0\}$$

Since $\mathbf{Z}$ is a PID, then for any ideal $\mathfrak{a} \in \mathbf{Z}$ with $\mathfrak{a} \neq 0$ and $\mathfrak{a} \neq \mathbf{Z}$, there exists a unique $m \geq 2 \in \mathbf{N}$ such that $\mathfrak{a} = m\mathbf{Z}$. For m, by the fundamental theorem of arithmetic, there exists a unique prime factorization

$$m = p_1^{e_1} \cdots p_k^{e_k}, \quad e_i \geq 1.$$

Then we know that for all $1 \leq i \leq k$, the ideal $\mathfrak{p}_i = p_i\mathbf{Z} \in \text{Spec}\mathbf{Z}$ and

$$V(\mathfrak{a}) = V(m\mathbf{Z}) = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_k\}.$$

That is to say that nontrivial closed sets in Spec $\mathbf{Z}$ is a finite collection of prime ideals in $\mathbf{Z}$. On the other hand, for any finite collection of prime ideals $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_k\}$ in $\mathbf{Z}$, for each $1 \leq i \leq k$, there exists a unique prime number $p_i \in \mathbf{Z}$ such that $\mathfrak{p}_i = p_i\mathbf{Z}$. Let $m = p_1 \cdots p_k$, and $\mathfrak{a} = m\mathbf{Z}$, then

$$V(m\mathbf{Z}) = V(\mathfrak{a}) = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_k\}.$$

So we know that a subset U of Spec $\mathbf{Z}$ is open if and only if $U = \emptyset$ or Spec $\mathbf{Z}\backslash U$ is a finite set. That is to say, the topology on Spec $\mathbf{Z}$ is the finite completion topology.

b. For $\mathbf{R}$, since $\mathbf{R}$ is a field, then only prime ideal in $\mathbf{R}$ is 0, that is,

$$\text{Spec } \mathbf{R} = \{0\}.$$

The open sets of Spec $\mathbf{R}$ are $\emptyset$ and $\{0\}$, and the topology on Spec $\mathbf{R}$ is the discrete topology.

c. For $\mathbf{C}[x]$, since $\mathbf{C}[x]$ is PID, then the ideal $\mathfrak{p}$ of $\mathbf{C}[x]$ is prime if and only if $\mathfrak{p} = 0$ or $\mathfrak{p} = f(x)\mathbf{C}[x]$ for some monic irreducible polynomial $f(x) \in \mathbf{C}[x]$ with $\text{deg}f(x) \geq 1$. Since $\mathbf{C}$ is algebraic closed, then only monic irreducible polynomials are of the form $x - c$ for some $c \in \mathbf{C}$. Hence we know that

$$\text{Spec } \mathbf{C}[x] = \{\mathfrak{p} : \mathfrak{p} = 0 \text{ or } \mathfrak{p} = (x - c)\mathbf{C}[x] \text{ for some } c \in \mathbf{C}\}.$$

Since $\mathbf{C}[x]$ is a PID, then for any ideal $\mathfrak{a} \in \mathbf{C}[x]$ with $\mathfrak{a} \neq 0$ and $\mathfrak{a} \neq \mathbf{C}[x]$, there exists a unique monic polynomial $m(x) \in \mathbf{C}[x]$ such that $\mathfrak{a} = m(x)\mathbf{C}[x]$. For $m(x)$, since $\mathbf{C}[x]$ is UFD, then there exists some $c_1, c_2, \cdots, c_k \in \mathbf{C}$ such that

$$m(x) = (x - c_1)^{e_1} \cdots (x - c_k)^{e_k}, \quad e_i \geq 1.$$

Then we know that for all $1 \leq i \leq k$, the ideal $\mathfrak{p}_i = (x - c_i)\mathbf{C}[x] \in \text{Spec}\mathbf{C}[x]$ and

$$V(\mathfrak{a}) = V(m(x)\mathbf{C}[x]) = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_k\}.$$

That is to say that nontrivial closed sets in Spec $\mathbf{C}[x]$ is a finite collection of prime ideals in $\mathbf{C}[x]$. On the other hand, for any finite collection of prime ideals $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_k\}$ in $\mathbf{C}[x]$, for each $1 \leq i \leq k$, there exists a unique $c_i \in \mathbf{C}$ such that $\mathfrak{p}_i = (x - c_i)\mathbf{C}[x]$. Let $m(x) = (x - c_1) \cdots (x - c_k)$, and $\mathfrak{a} = m(x)\mathbf{C}[x]$, then

$$V(m(x)\mathbf{C}[x]) = V(\mathfrak{a}) = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_k\}.$$

So we know that a subset U of Spec $\mathbf{C}[x]$ is open if and only if $U = \emptyset$ or Spec $\mathbf{C}[x]\backslash U$ is a finite set. That is to say, the topology on Spec $\mathbf{C}[x]$ is the finite completion topology.

d. For $\mathbf{R}[x]$, since $\mathbf{R}[x]$ is PID, then the ideal $\mathfrak{p}$ of $\mathbf{R}[x]$ is prime if and only if $\mathfrak{p} = 0$ or $\mathfrak{p} = f(x)\mathbf{R}[x]$ for some monic irreducible polynomial $f(x) \in \mathbf{R}[x]$ with $\text{deg}f(x) \geq 1$. Since only monic irreducible polynomials are of the form $x - c$ for some $c \in \mathbf{R}$ or $x^2 + ax + b$ with $a^2 - 4b < 0$ for some $a, b \in \mathbf{R}$. Hence we know that

$$\text{Spec } \mathbf{R}[x] = \{\mathfrak{p} : \mathfrak{p} = 0 \text{ or } \mathfrak{p} = (x - c)\mathbf{R}[x] \text{ for } c \in \mathbf{R} \text{ or } \mathfrak{p} = (x^2 + ax + b)\mathbf{R}[x] \text{ for } a, b \in \mathbf{R} \text{ with } a^2 - 4b < 0\}.$$

Since $\mathbf{R}[x]$ is a PID, then for any ideal $\mathfrak{a} \in \mathbf{R}[x]$ with $\mathfrak{a} \neq 0$ and $\mathfrak{a} \neq \mathbf{R}[x]$, there exists a unique monic polynomial $m(x) \in \mathbf{R}[x]$ such that $\mathfrak{a} = m(x)\mathbf{R}[x]$. For $m(x)$, since $\mathbf{R}[x]$ is UFD, then there exists some irreducible monic polynomials $p_1(x), \cdots, p_k(x) \in \mathbf{R}[x]$ such that

$$m(x) = p_1(x)^{e_1} \cdots p_k(x)^{e_k}, \quad e_i \geq 1.$$

Then we know that for all $1 \leq i \leq k$, the ideal $\mathfrak{p}_i = p_1(x)\mathbf{R}[x] \in \mathrm{Spec}\mathbf{R}[x]$ and

$$V(\mathfrak{a}) = V(m(x)\mathbf{R}[x]) = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_k\}.$$

That is to say that nontrivial closed sets in Spec $\mathbf{R}[x]$ is a finite collection of prime ideals in $\mathbf{R}[x]$. On the other hand, for any finite collection of prime ideals $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_k\}$ in $\mathbf{R}[x]$, for each $1 \leq i \leq k$, there exists a unique monic irreducible polynomial $p_i(x) \in \mathbf{R}[x]$ such that $\mathfrak{p}_i = p_i(x)\mathbf{R}[x]$. Let $m(x) = p_1(x) \cdots p_k(x)$, and $\mathfrak{a} = m(x)\mathbf{R}[x]$, then

$$V(m(x)\mathbf{R}[x]) = V(\mathfrak{a}) = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_k\}.$$

So we know that a subset U of Spec $\mathbf{R}[x]$ is open if and only if $U = \emptyset$ or Spec $\mathbf{R}[x] \backslash U$ is a finite set. That is to say, the topology on Spec $\mathbf{R}[x]$ is the finite completion topology.

e. Claim I: The ideal $\mathfrak{p}$ of $\mathbf{Z}[x]$ is prime if and only if $\mathfrak{p}$ is one of the following cases:

i. $\mathfrak{p} = 0$.
ii. $\mathfrak{p} = (p)$ for some prime number p in $\mathbf{Z}$.
iii. $\mathfrak{p} = (f(x))$ for some primitive irreducible polynomial $f(x)$ in $\mathbf{Z}[x]$.
iv. $\mathfrak{p} = (p, f(x))$ for some prime number p in $\mathbf{Z}$ and primitive irreducible polynomial $f(x)$ in $\mathbf{Z}[x]$ such that $f(x)$ is also irreducible in $\mathbf{Z}[x]/p\mathbf{Z}[x] \cong \mathbf{F}_p[x]$.

($\Longleftarrow$) i. Since $\mathbf{Z}[x]$ is a domain, then $\mathfrak{p} = 0$ is prime in $[Z][x]$.

ii. For any $f(x), g(x) \in \mathbf{Z}[x]$ such that $f(x)g(x) \in \mathfrak{p} = (p)$ for some prime number p in $\mathbf{Z}$, then

$$p | f(x)g(x)$$

Recall the Gauss's Lemma:

Let A be a UFD, $f(x)$ and $g(x)$ be primitive plolynomials in $A[X]$, then $f(x)g(x)$ is also primitive.

Since p is a prime number in $\mathbf{Z}$, by the Gauss's Lemma, we know that $p|f(x)$ or $p|g(x)$ in $\mathbf{Z}[x]$, that is, $f(x) \in \mathfrak{p}$ or $g(x) \in \mathfrak{p}$. Hence $\mathfrak{p}$ is prime in $\mathbf{Z}[x]$.

iii. For any $g(x), h(x) \in \mathbf{Z}[x]$ such that $g(x)h(x) \in \mathfrak{p} = (f(x))$ for some primitive irreducible polynomial $f(x)$ in $\mathbf{Z}[x]$, then

$$f(x) | g(x)h(x)$$

Since $f(x)$ is irreducible in $\mathbf{Z}[x]$, then $f(x)$ is also irreducible in $\mathbf{Q}[x]$. Hence $f(x)|g(x)$ or $f(x)|h(x)$ in $\mathbf{Q}[x]$. Without loss of generality, assume $f(x)|g(x)$ in $\mathbf{Q}[x]$, then there exists some $m(x) \in \mathbf{Q}[x]$ such that

$$g(x) = m(x)f(x).$$

Since $f(x), g(x) \in \mathbf{Z}[x]$ and f is primitive, by the Gauss's Lemma, then $m(x) \in \mathbf{Z}[x]$, that is, $f(x)|g(x)$ in $\mathbf{Z}[x]$. Hence $\mathfrak{p}$ is prime in $\mathbf{Z}[x]$.

iv. $\mathfrak{p} = (p, f(x))$ for some prime number p in $\mathbf{Z}$ and primitive irreducible polynomial $f(x)$ in $\mathbf{Z}[x]$ such that $f(x)$ is also irreducible in $\mathbf{Z}/p\mathbf{Z}[x]$. Let $\pi : \mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ be the natural ring homomorphism, that is, for all $n \in \mathbf{Z}$, we have

$$\pi(n) = n + p\mathbf{Z}.$$

Then π can induce a ring homomorphism $\overline{\pi} : \mathbf{Z}[x] \to \mathbf{Z}/p\mathbf{Z}[x]$ such that $\overline{\pi}|_{\mathbf{Z}} = \pi$. Since $\mathbf{Z}/p\mathbf{Z}$ is a field and $\overline{f}(x)$ is irreducible on $\mathbf{Z}/p\mathbf{Z}[x]$, then $\mathbf{Z}/p\mathbf{Z}[x]/(\overline{f(x)})$ is a field extension of $\mathbf{Z}/p\mathbf{Z}$.

Define the map $\Phi : \mathbf{Z}[x] \to \mathbf{Z}/p\mathbf{Z}[x]/(\overline{f(x)})$ as: for all $g(x) \in \mathbf{Z}[x]$, we have

$$\Phi(g(x)) = \overline{g(x)} + (\overline{f(x)}).$$

It is easy to see that Φ is a ring homomorphism. Now let's look at the kernel of Φ. It is easy to see that $p, f(x) \in \ker \Phi$, since $\ker \Phi$ is an ideal of $\mathbf{Z}[x]$, then

$$(p, f(x)) \subset \ker \Phi.$$

On the other hand, for all $g(x) \in \ker \Phi$, then $\overline{g(x)} \in (\overline{f(x)})$. That is, there exists some $h \in \mathbf{Z}[x]$ such that

$$\overline{g(x)} = \overline{f(x)}\overline{h(x)} = \overline{f(x)h(x)}$$

Hence $\overline{g(x) - f(x)h(x)} = 0$, that is, there exists some $k(x) \in \mathbf{Z}[x]$ such that

$$g(x) - f(x)h(x) = pk(x).$$

That is, $g(x) = h(x)f(x) + k(x)p \in (p, f(x))$. Hence we get

$$\ker \Phi = (p, f(x)).$$

By the first isomorphism theorem, then

$$\mathbf{Z}/p\mathbf{Z}[x]/(\overline{f(x)}) \cong \mathbf{Z}[x]/(p, f(x)),$$

which is a field. Hence $(p, f(x))$ is maximal in $\mathbf{Z}[x]$, in particular, $\mathfrak{p} = (p, f(x))$ is prime in $\mathbf{Z}[x]$.

($\Longrightarrow$) Now assume $\mathfrak{p}$ is a prime ideal in $\mathbf{Z}[x]$. If $\mathfrak{p} = 0$, we are done. Now assume $\mathfrak{p} \neq 0$. Let $\mathfrak{q} = \mathfrak{p} \bigcap \mathbf{Z}$, then $\mathfrak{q}$ is prime in $\mathbf{Z}$.

Case I: If $\mathfrak{q} = 0$. Let $S = \mathbf{Z} \backslash \{0\}$, then S is a multiplicative subset of $\mathbf{Z}[x]$ and $\mathfrak{p} \bigcap S = \emptyset$. Since $S^{-1}\mathbf{Z} = \mathbf{Q}$, then

$$S^{-1}\mathbf{Z}[x] = \mathbf{Q}[x].$$

Since $S \bigcap \mathfrak{p} = \emptyset$ and $\mathfrak{p}$ is prime in $\mathbf{Z}[x]$, then $S^{-1}\mathfrak{p}$ is prime in $S^{-1}\mathbf{Z}[x] = \mathbf{Q}[x]$. Since $\mathbf{Q}[x]$ is PID, then there exists some irreducible polynomial $f(x) \in \mathbf{Q}[x]$ such that $S^{-1}\mathfrak{p} = (f(x))$ in $\mathbf{Q}[x]$. Then by multiplying some constant, without loss of generality, we can assume $f(x) \in \mathbf{Z}[x]$. Since $\mathfrak{p} \bigcap S = \emptyset$, then

$$\mathfrak{p} = (f(x)) \bigcap \mathbf{Z}[x].$$

That is, $\mathfrak{p} = (f(x))$ in $\mathbf{Z}[x]$, where $f(x)$ is primitive irreducible polynomial in $\mathbf{Z}[x]$.

Case II: If $\mathfrak{q} \neq 0$. Since $\mathfrak{q}$ is prime in $\mathbf{Z}$, then there exists some prime number p in $\mathbb{Z}$ such that $\mathfrak{q} = p\mathbf{Z}$, then $p\mathbf{Z}[x] \subset \mathfrak{p}$. By the forth isomorphism theorem, we know that $\mathfrak{p}/p\mathbf{Z}[x]$ is a prime ideal in $\mathbf{Z}[x]/p\mathbf{Z}[x] = \mathbf{Z}/p\mathbf{Z}[x]$. Since $\mathbf{Z}/p\mathbf{Z}$ is a field, then $\mathbf{Z}[x]/p\mathbf{Z}[x] = \mathbf{Z}/p\mathbf{Z}[x]$ is PID.

Subcase I: $\mathfrak{p}/p\mathbf{Z}[x] = 0$, then $\mathfrak{p} = (p)$, we are done.

Subcase II: $\mathfrak{p}/p\mathbf{Z}[x] \neq 0$, since $\mathfrak{p}/p\mathbf{Z}[x]$ is a prime ideal in $\mathbf{Z}[x]/p\mathbf{Z}[x] = \mathbf{Z}/p\mathbf{Z}[x]$ which is PID, then there exists some primitive irreducible polynomial $f(x) \in \mathbf{Z}[x]$ such that $\overline{f(x)}$ is irreducible in $\mathbf{Z}/p\mathbf{Z}[x]$ and

$$\mathfrak{p}/p\mathbf{Z}[x] = (\overline{f(x)}).$$

Hence we get $\mathfrak{p} = (p, f(x))$.

In summary, we can conclude that the Claim I is true.

$\square$

(Mingfeng Zhao) Department of Mathematics, University of Connecticut, 196 Auditorium Road, Unit 3009, Storrs, CT 06269-3009

E-mail address: `mingfeng.zhao@uconn.edu`