Arithmetic Geometry Problems

Theo Koss

October 2024

1 Chapter 1

1. Let $d \in \mathbb{Q} \setminus \mathbb{Z}$, prove $\mathbb{Z}[\sqrt{d}]$ is not a finitely generated abelian group.

   Proof. Let $d = \frac{p}{q}$ with $p \neq q \in \mathbb{Z},\ q \neq 0, 1$ and $\gcd(p, q) = 1$. Note that subgroups of finitely generated *abelian* groups are themselves finitely generated. So consider $\mathbb{Z}[d] < \mathbb{Z}[\sqrt{d}]$. Assume BWOC that $\mathbb{Z}[d]$ is finitely generated, say n generators. Then we can write any element of $\mathbb{Z}[d]$ as a linear combination of these elements. Consider

$$\begin{aligned}
\frac{1}{q^{n+1}} &= b_0 + b_1 d + b_2 d^2 + \cdots + b_n d^n && \text{(For integers } b_i\text{)} \\
&= b_0 + b_1 \frac{p}{q} + \cdots + b_n \frac{p^n}{q^n} \\
\implies 1 &= b_0 \cdot q^{n+1} + b_1 p \cdot q^n + \cdots + b_n p^n \cdot q \\
&= q \underbrace{\left(b_0 \cdot q^n + b_1 p \cdot q^{n-1} + \cdots + b_n p^n\right)}_{\in \mathbb{Z}} \\
\implies \frac{1}{q} &\in \mathbb{Z}
\end{aligned}$$

   Contradiction because we have $q \neq 1$. □

   Alternate Proof: Proposition 2.10 in the book, the $\mathbb{Z}$-module $\mathbb{Z}[x]$ is finitely generated iff x is algebraic over $\mathbb{Z}$. We have minimal polynomial:

$$m_{\sqrt{d},\mathbb{Z}}(x) = x^2 - d = qx^2 - p$$

Which is not monic in $\mathbb{Z}$ because we have $q \neq 1$ and q does not divide p. $\square$

2. Prove $\mathbb{Z}[\frac{2+i}{5}] \cap \mathbb{Q} = \mathbb{Z}$ and $\mathbb{Z}[\frac{2-i}{5}] \cap \mathbb{Q} = \mathbb{Z}$.

   Proof. Assume, BWOC, that we have some element $k \in \mathbb{Z}[\frac{2+i}{5}]$ such that $k \in \mathbb{Q} \setminus \mathbb{Z}$. Then $k = \frac{p}{q}$ with $p, q \in \mathbb{Z}$, $q \neq 0, 1$ and $\gcd(p, q) = 1$. We also have
$$k = a + b \cdot \frac{2+i}{5} = a + \frac{2b}{5} + \frac{bi}{5}$$
   for some $a, b \in \mathbb{Z}$. Since $k = \frac{p}{q}$ is strictly real, we must have
$$\frac{bi}{5} = 0 \implies b = 0$$
   But then $k = a + 0 \in \mathbb{Z}$ contradiction.
   Similarly, write $k = a + b \cdot \frac{2-i}{5} = a + \frac{2b}{5} - \frac{bi}{5}$ so $\frac{bi}{5} = 0 \implies b = 0$ so $k \in \mathbb{Z}$. $\square$

3. Let A be a ring, and let I, J be two coprime ideals of A. Show that, $\forall a, b \in \mathbb{N},\ I^a$ is coprime to J^b.

   Proof. Since I and J are coprime, by definition we have $I + J = A$. Base case: $I^1 + J^1 = A$ obviously. Fix some $b \in \mathbb{N}$, assume I^k is coprime to J^n, for some $a \in \mathbb{N}$. Then
$$I^a + J^b = A$$
   Multiply both sides by I (on the left),
$$I^{a+1} + J^b = IA = A$$
   Thus I^{a+1} is coprime to J^b. Therefore the statement is true for all pairs $a, b \in \mathbb{N}$. $\square$

4. Show that in the ring $\mathbb{Z}[\sqrt{-5}]$, the elements $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are irreducible, and that they are not associates.

5. Let p be a prime number. Let $\bar{g}(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ be any irreducible polynomial. Let $g(x) \in \mathbb{Z}[x]$ be such that its image under the natural reduction map $\mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$ is $\bar{g}(x)$. Show that the ideal $(p, g(x))$ is a maximal ideal of $\mathbb{Z}[x]$.

   Proof. We have that

$$\mathbb{Z}[x]/(p, g(x)) \cong (\mathbb{Z}[x]/p)/(g(x)) \cong (\mathbb{Z}/p\mathbb{Z})[x]/(g(x))$$

   Then, consider the natural reduction map

$$\pi : \mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$$

   And we have $\pi(g(x)) = \bar{g}(x)$, so $(\mathbb{Z}/p\mathbb{Z})[x]/(g(x)) \cong (\mathbb{Z}/p\mathbb{Z})[x]/(\bar{g}(x))$. We know $\bar{g}(x)$ is irreducible, and the ring $(\mathbb{Z}/p\mathbb{Z})[x]$ is a PID, so the ideal $(\bar{g}(x))$ is maximal, and therefore $(\mathbb{Z}/p\mathbb{Z})[x]/(\bar{g}(x))$is a field, (finite field $\mathbb{F}_{p^{\deg(\bar{g}(x))}}$). So the ideal $(p, g(x))$ is maximal in $\mathbb{Z}[x]$ □

6. Show that a prinicpal ideal domain has the property of unique factorization of ideals.

   Proof. Let A be a PID, then it is also a UFD. Consider an arbitrary ideal $I = (a) \subset A$, then, by UFD, a can be written uniquely as a product of irreducibles, $a = p_1 \cdots p_n$. But, since every ideal is principal, and every element is contained in the ideal generated by it, we have

$$I = (a) = (p_1) \cdots (p_n)$$

   And in a PID, ideals generated by irreducibles are maximal, and maximal = prime. So we have a unique factorization of the ideal I into prime ideals. □

7. Let A be a commutative ring and $I \subset A$ be an ideal.

   (a). Let $a_1, \ldots, a_s \in A$ and let J denote the ideal of A/I generated by the images of $a_1, \ldots, a_s$ under the map $A \to A/I$. Show that

$$(A/I)/J \xrightarrow{\sim} A/(I, a_1, \ldots, a_s)$$

Proof. We have the natural homomorphism $\pi : A \to A/I$, and we have another homomorphism $\psi : A/I \to (A/I)/J$ which has $\ker(\psi) = J = (\pi(a_1), \dots, \pi(a_s))$. COME BACK! $\square$

(b). Let J be any ideal of A. Show that

$$(A/I)/(J + I/I) \cong (A/J)/(I + J/J)$$

Proof. $\square$

(c).

8. (a). Let k be any field. Let $A := k[x_1, \dots, x_n, \dots]$ be the polynomial ring in countably many variables. Show that A is not Noetherian.

Proof. By way of contradiction, assume A is Noetherian, so every increasing chain of ideals

$$I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_n = I_{n+1}$$

Stabilizes at some point. We have the ideals

$$(x_1) \subset (x_1, x_2) \subset \dots (x_1, \dots, x_n) = (x_1, \dots, x_n, x_{n+1})$$

That gives $x_{n+1} \in I_n = (x_1, \dots, x_n)$. So we can write x_{n+1} as a linear combination of the elements of that ideal,

$$x_{n+1} = \sum_{i=1}^{n} c_i x_i$$

But, consider the evaluation mapping $\phi : A \to k$ by evaluating $x_1, \dots, x_n = 0$ and $x_{n+1} = 1$. Applying this evaluation mapping to above gives

$$1 = \phi(x_{n+1}) = \phi(\sum_{i=1}^{n} c_i x_i) = \sum c_i \phi(x_i) = \sum c_i \cdot 0 = 0$$

Contradiction. $\square$

(b). Let $\bar{\mathbb{Q}}$ denote an algebraic closure of $\mathbb{Q}$. Let $\mathcal{O}$ denote the integral closure of $\mathbb{Z}$ in $\bar{\mathbb{Q}}$. Show that $\mathcal{O}$ is not a Noetherian ring. (Hint: find a nonstationary sequence of ideals in $\mathcal{O}$ by taking successive roots of an integer.)

Proof. Let $\mathcal{O}$ be the integral closure of $\mathbb{Z}$ in $\bar{\mathbb{Q}}$. Then in particular, $\mathbb{Z} \subset \mathcal{O}$, so consider $2 \in \mathcal{O}$. Let $I = (2)$. Then consider the increasing chain of ideals:

$$I = (2) \subset (\sqrt{2}) \subset (\sqrt[3]{2}) \subset \cdots \subset \sqrt{I}$$

Each ideal strictly contains the next, so this is a nonstationary increasing chain of ideals. (Equivalently the radical is not finitely generated) $\square$

9. Let k be a field, and $A := k[x_1, \dots, x_n]$. Let $\bar{k}$ denote an algebraic closure of k, and let $B := \bar{k}[x_1, \dots, x_n]$. Show that the extension B/A is integral. Note that in general, B is not a finitely generated A-module.

   Proof. B/A is integral iff every element of B is integral over A (is the root of a monic polynomial in $A[y]$). So, choose an arbitrary element $\alpha \in B$. There are two cases:

   (a) If $\alpha \in A$, then we are done because $y - \alpha$ is a polynomial in $A[y]$ that is satisfied by α.

   (b) So, assume $\alpha \in B - A$. Then, since $\bar{k}$ is an algebraic closure of k, for all $\beta \in \bar{k}$, we have $f(\beta) = 0$ where f is a monic polynomial with coefficients in k. So, let $\alpha \in B$, then

   $$\alpha = \sum_{i=1}^{n} c_i x_i^{a_i}$$

   Where $c_i \in \bar{k}$. Since $\bar{k}$ is an algebraic closure, for each coefficient c_i, there exists a monic polynomial $p_i \in A$ such that $p_i(c_i) = 0$. Then, the product of all of these p_i kills each coefficient, so let

   $$A \ni P(x_1, \dots, x_n) = \prod_{i=1}^{n} p_i(x_i)$$

   Then

   $$P(\alpha) = P\left(\sum_{i=1}^{n} c_i x_i^{a_i}\right) = \prod_{i=1}^{n} p_i \left(\sum_{i=1}^{n} c_i x_i^{a_i}\right) = 0$$

   And, a product of monic polynomials is monic, so $P(x_1, \dots, x_n)$ is a monic polynomial in A which is satisfied by α as required.

□

10. Let B/A be an integral extension. Show that B is a field iff A is a field.

    Proof. ($\implies$) Let B/A be an integral extension and B be a field. Let $a \in A - \{0\}$, then by definition of extension, $a \in B$ and $a^{-1} \in B$ since B is a field. Since B is integral over A, $\exists g(y) \in A[y]$ with $g(a^{-1}) = 0$, and $g(y)$ monic. Multiply

    $$g(a^{-1}) = (a^{-1})^n + a_{n-1}(a^{-1})^{n-1} + \cdots + a_1(a^{-1}) + a_0 = 0$$

    by a^n, so

    $$1 + a_{n-1}a + \cdots + a_1 a^{n-1} + a_0 a^n = 0$$

    which gives

    $$a_{n-1}a + \cdots + a_1 a^{n-1} + a_0 a^n = -1$$

    as a polynomial in $A[a]$. Since we have a linear combination in $A[a]$ which equals -1, we also have a linear combination in $A[a]$ which equals 1, and so $a^{-1} \in A$ so A is a field.

    ($\impliedby$) Let B/A be an integral extension and A a field. Then B/A is a field extension, and so B is a field. □

11. Let B/A be an integral extension. Let $M \subset B$ be a prime ideal. Let $P := M \cap A$. Show that M is maximal in B iff P is maximal in A.

    Proof. ($\implies$) Let M be maximal in B. Then B/M is a field and $(B/M)/(A/P)$ an integral extension obtained by restricting the extension B/A. So by the problem above, A/P is a field, so that $P \subset A$ is a maximal ideal of A.

    ($\impliedby$) Let $P = M \cap A$ be a maximal ideal of A. Then A/P is a field and then by above, B/M is also a field so $M \subset B$ is a maximal ideal. □

13. Let A be a PID with field of fractions K. Let L/K be an extension of degree 2. Assume that the integral closure B of A in L is a finitely generated A-module. Show that there exists $b \in B$ such that $\{1, b\}$ is a basis for B over A.

Proof. Consider an element $z \in B$. We want to show that there exists a $b \in B$ so that $z = 1a_0 + ba_1$ for some $a_i \in A$. Since B is the integral closure of A, z satisfies a monic polynomial $g(y) \in A[y]$. And since L/K is a degree 2 extension, g has degree at most 2. If the degree of g is 1, then $z \in A$ and so $z = 1 \cdot z$ is its linear combination. So assume $\deg(g) = 2$,

$$g(y) = y^2 + c_1 y + c_0$$

With $c_i \in A$. By definition,

$$g(z) = 0 = z^2 + c_1 z + c_0$$

Since $z \in B \subset L$, we have $z = \frac{r}{s}$, $r, s \in B$ and $s \neq 0$.

$$0 = \left(\frac{r}{s}\right)^2 + \frac{c_1 r}{s} + c_0$$

Multiplying by s^2:

$$0 = r^2 + c_1 rs + c_0 s^2$$

(COME BACK) □

2 Chapter 2

1. Let A be a local ring with maximal ideal M. Let $m \in M$ and $a \in A - M$. Show that $a + m$ is a unit in A.

   Proof. Assume $a + m$ is a non-unit, then by Zorn's lemma, $a + m$ is contained in a maximal ideal, but there is only one maximal ideal, so $a + m \in M \implies a \in M$ contradiction, so $a + m$ must be a unit. □

2. Show that a ring A is a local ring iff the complement in A of the set of units A^* is an ideal of A.

   Proof. ($\implies$) Let A be a local ring, and M its unique maximal ideal. Then by Zorn's lemma, $\forall x \in A - A^*$, $x \in M$ so $A - A^* = M$ is a (maximal) ideal of A.

($\Longleftarrow$) Let A be a ring such that $M := A - A^*$ is an ideal of A. Let I be an ideal, then I contains no units, otherwise $I = A$, so then $I \subseteq A - A^* = M$. Then each ideal I is contained in M, so M is the unique maximal ideal of A, which means A is local. $\square$

3. Let A be a local ring with maximal ideal $\mathcal{M}$. If M is any A-module, let $\mathcal{M}M := \{\sum_{i=1}^n \mu_i m_i \mid \mu_i \in \mathcal{M},\ m_i \in M,\ n \in \mathbb{N}\}$. $\mathcal{M}M$ is an A-submodule of M. Assume now that M is a finitely generated A-module. Show that if $\mathcal{M}M = M$, then $M = (0)$. Hint: Let $\{m_1, \dots, m_n\}$ be a system of generators for M. Express that $m_i \in \mathcal{M}M$ and use problem 1.

   Proof. Let M be a finitely generated A-module and assume $\mathcal{M}M = M$, so

$$\begin{aligned}\mathcal{M}M &:= \left\{\sum_{i=1}^{n} \mu_i m_i \mid \mu_i \in \mathcal{M},\ m_i \in M,\ n \in \mathbb{N}\right\}\\ &= \left\{\sum_{j=1}^{n} a_j m_j \mid a_j \in A,\ m_j \in M,\ n \in N\right\}\end{aligned}$$

   Let $x \in M$, then x is a linear combination of the basis $\{m_1, \dots, m_n\}$ with coefficients from $\mathcal{M}$ and with coefficients from A:

$$\begin{aligned} x &= \mu_1 m_1 + \mu_2 m_2 + \dots + \mu_n m_n\\ x &= a_1 m_1 + a_2 m_2 + \dots + a_n m_n\\ \Longrightarrow\ 0 &= (a_1 - \mu_1)m_1 + \dots + (a_n - \mu_n)m_n\end{aligned}$$

   Since $\{m_1, \dots, m_n\}$ is a basis, we have either $(a_i - \mu_i) = 0$ or $m_i = 0$ for all $i \in \{1, \dots, n\}$. However, by problem 1, any element of the form $a + m$ for $a \in A$ and $m \in \mathcal{M}$ is a unit, so $a_i - \mu_i \neq 0$ which means $m_i = 0$ for all i, and so $M = (0)$. $\square$

4. Let A and B be two local principal ideal domains with the same field of fractions. Show that if $A \subseteq B$, then $A = B$. (Maybe have to assume B is not the field of fractions)

Proof. Let A be a local PID and $M \subset A$ its unique maximal (therefore prime) ideal. Let K be the field of fractions of both A and B. We have $A \subseteq B \subseteq K$.

claim: Every ring between a PID A and its field of fractions K is a localization of A.

Proof of claim. See proposition 6.4 (Universal property of rings of fractions) $\square$

So now because $A \subseteq B \subseteq K$ and A is a PID, the choices for B are all the localizations of A. If we choose $T = A - \{0\}$, then $T^{-1}A = B = K$ contradiction. So we must choose the only other multiplicative set, $S = A - M$, then $B = S^{-1}A$. The units in B are then just elements of the form $b = 1/s$ so $s \in B$ is also a unit, but $s \in A$ is a unit because it is in $A - M$ (problem 1). So $A = B$. $\square$

5. Let A be a domain with field of fractions $K = A_{(0)}$. Let M be any A-module. The rank of M over K, denoted by $\text{rank}_A(M)$, is the dimension of the K-vector space $M_{(0)}$.

   (a). Show that M is a torsion A-module iff $\text{rank}_A(M) = 0$.

   (b). Let
   $$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$
   be an exact sequence of A-modules. Show that $\text{rank}_A(M) < \infty$ iff $\text{rank}_A(M') < \infty$ and $\text{rank}_A(M'') < \infty$. Show that if $\text{rank}_A(M) < \infty$, then $\text{rank}_A(M) = \text{rank}_A(M') + \text{rank}_A(M'')$. In particular, show that $\text{rank}_A(M_1 \oplus M_2) = \text{rank}_A(M_1) + \text{rank}_A(M_2)$.

Proof. (a). ($\implies$) Let M be a torsion A-module, so that $\forall m \in M$, $\exists a \neq 0 \in A$ with $am = 0$. Note that $M_{(0)}$ is the K-vector space obtained by extending scalars from A to K, so $M_{(0)} = K \otimes_A M$ then consider $\mathfrak{m} \in M$

$$\mathfrak{m} = k \otimes m = \frac{1}{a} \otimes am = \frac{1}{a} \otimes 0 = 0$$

So $M_{(0)} = \{0\}$ and thus is a 0 dimensional K-vector space.

($\Longleftarrow$) Let M be an A-module with rank 0. So

$$M_{(0)} = \{0\} = K \otimes_A M$$

Therefore we have some nonzero $k \in K$ which annihilates M. Let $k = \frac{a}{b}$ be such that $\frac{a}{b} \otimes m = 0$ for all $m \in M$.

$$0 = \frac{a}{b} \otimes m = \frac{1}{b} \otimes am$$

Clearly $\frac{1}{b} \neq 0$, so $am = 0$, we also have that $k = \frac{a}{b}$ was nonzero so that a is not 0. Therefore we have a nonzero $a \in A$ such that $\forall m \in M$, $am = 0$. Thus M is a torsion A-module.

(b). Let

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

Be an exact sequence of A-modules, then (since field of fractions is a flat module)

$$0 \longrightarrow K \otimes_A M' \xrightarrow{1 \otimes f} K \otimes_A M \xrightarrow{1 \otimes g} K \otimes_A M'' \longrightarrow 0$$

is exact. Let $M_{(0)} := K \otimes_A M$ and $\bar{h} := 1 \otimes h$. By the first isomorphism theorem for modules (in this case K-vector spaces), $M_{(0)}/\ker(\bar{g}) \cong M''_{(0)}$. Since $\ker(\bar{g}) = \operatorname{im}(\bar{f}) = M'_{(0)}$ by exactness,

$$M_{(0)}/M'_{(0)} \cong M''_{(0)}$$

Then

$$\operatorname{rank}_A(M) = \operatorname{rank}_A(M') + \operatorname{rank}_A(M'')$$

(i) ($\Longrightarrow$) Let $\operatorname{rank}(M)$ be finite. Then neither $\operatorname{rank}(M')$ nor $\operatorname{rank}(M'')$ can be infinite.

(ii) ($\Longleftarrow$) Let $\operatorname{rank}(M'')$ and $\operatorname{rank}(M'')$ be finite, then their sum is finite so $\operatorname{rank}(M) < \infty$.

(iii) Let M_1 and M_2 be A-modules. Then $M_1 \oplus M_2$ is an A-module and we have a natural short (split) exact sequence

$$0 \longrightarrow M_1 \xrightarrow{\imath} M_1 \oplus M_2 \xrightarrow{\phi} M_2 \longrightarrow 0$$

Where $\imath : M_1 \hookrightarrow M_1 \oplus M_2$ is the inclusion map, and $\phi : M_1 \oplus M_2 \to M_2$ is the projection. Clearly $\mathrm{im}(\imath) = M_1$ as it is an injection, and $\ker(\phi) = \{(m_1, 0) \mid m_1 \in M_1\} = M_1$. Then, we can tensor this sequence with the flat module K to see

$$\mathrm{rank}(M_1 \oplus M_2) = \mathrm{rank}(M_1) + \mathrm{rank}(M_2)$$

$\square$

6. Let A be a commutative domain. Let M be an A-module. Let $(0) = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_{s-1} \subseteq M_s = M$ be a chain of A-submodules. Assume that $\mathrm{rank}(M_i/M_{i-1})$ is finite, $\forall i = 1, 2, \ldots, s$. Show that

$$\mathrm{rank}(M) = \sum_{i=1}^{s} \mathrm{rank}(M_i/M_{i-1})$$

Proof. This chain of A-submodules gives natural injections $\imath_n : M_n \to M_{n+1}$. Each injection defines a short exact sequence:

$$0 \longrightarrow M_n \xrightarrow{\imath} M_{n+1} \longrightarrow M_{n+1}/M_n \longrightarrow 0$$

Tensoring each sequence with the field of fractions of A. Gives exact sequences

$$0 \longrightarrow \mathcal{M}_n \xrightarrow{\imath} \mathcal{M}_{n+1} \longrightarrow \mathcal{M}_{n+1}/\mathcal{M}_n \longrightarrow 0$$

Then since this is an exact sequence of vector spaces, it splits and so for each n, $\mathcal{M}_{n+1} \cong \mathcal{M}_n \oplus \mathcal{M}_{n+1}/\mathcal{M}_n$. In particular,

$$\begin{aligned}
\mathcal{M}_s &\cong [\mathcal{M}_{s-1} \oplus \mathcal{M}_s/\mathcal{M}_{s-1}] \\
&\cong [(\mathcal{M}_{s-2} \oplus \mathcal{M}_{s-1}/\mathcal{M}_{s-2}) \oplus \mathcal{M}_s/\mathcal{M}_{s-1}] \\
&\cong [(\mathcal{M}_{s-3} \oplus \mathcal{M}_{s-2}/\mathcal{M}_{s-3}) \oplus (\mathcal{M}_{s-1}/\mathcal{M}_{s-2}) \oplus \mathcal{M}_s/\mathcal{M}_{s-1}] \\
&\vdots \\
&\cong \bigoplus_{i=1}^{s} (\mathcal{M}_i/\mathcal{M}_{i-1})
\end{aligned}$$

Each term has $\dim_K(\mathcal{M}_i/\mathcal{M}_{i-1}) = \operatorname{rank}_A(M_i/M_{i-1})$ so

$$\operatorname{rank}_A(M) = \sum_{i=1}^{s} \operatorname{rank}_A(M_i/M_{i-1})$$

$\square$

7. Let A be a Noetherian domain with field of fractions K. Let $I \neq (0)$ be an ideal. Let $I^{-1} \coloneqq \{\alpha \in K \mid \alpha i \in A, \ \forall i \in I\}$. Show that I^{-1} is a finitely generated torsion free A-module of rank 1.

   Proof. First we will show that $I^{-1} \coloneqq \{\alpha \in K \mid \alpha i \in A, \ foralli \in I\}$ is indeed an A-module.

   - Let $\alpha, \beta \in I^{-1}$, then
   $$(\alpha + \beta)i = \alpha i + \beta i \in A \implies \alpha + \beta \in I^{-1}$$
   - Let $\alpha \in I^{-1}$, and $a \in A$ then
   $$(\alpha a)i = a(\alpha i) \in A$$
   So $\alpha a \in I^{-1}$

   So I^{-1} is an A-module. Then it defines a natural exact sequence of A-modules:

   $$0 \longrightarrow I^{-1} \longrightarrow A \longrightarrow A/(I^{-1}) \longrightarrow 0$$

   Notice that if $I \neq (0)$, then $I^{-1} \neq (0)$ and A/I^{-1} is torsion. Indeed, choose any $\alpha \in I^{-1}$, then $\alpha \neq 0 \in \operatorname{Ann}_A(A/I^{-1})$. So A/I^{-1} has a nonzero annihilator, and thus it is torsion. Now, tensoring the exact sequence with K, gives another exact sequence

   $$0 \longrightarrow K \otimes_A I^{-1} \longrightarrow K \longrightarrow K \otimes_A A/I^{-1} \longrightarrow 0$$

   So we have $\dim_K(K) = \dim_K(K \otimes_A I^{-1}) + \dim_K(K \otimes_A A/I^{-1})$. Clearly $\dim_K(K) = 1$, and by problem 5, $\operatorname{rank}_A(A/I^{-1}) = 0$ as A/I^{-1} is torsion. Therefore $K \otimes I^{-1} \cong K$ so I^{-1} is a torsion free A-module of rank 1. Notice if $I = (i)$ is the generator of I in A, then $I^{-1} = (\frac{1}{i})$ is the generator of I^{-1} in K, so I^{-1} is indeed finitely generated. $\square$

8. (a). Show that if $a, b \in \mathbb{Z}$, and $\gcd(a, b) = 1$, then $\mathbb{Z}[\frac{a}{b}] = \mathbb{Z}[\frac{1}{b}]$.
   (b). Show that any subring of $\mathbb{Q}$ that contains 1 is Noetherian.

   (a). *Proof.* Let $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$.

   - **Claim:** $\mathbb{Z}[\frac{1}{b}] \subseteq \mathbb{Z}[\frac{a}{b}]$
     By Bezout's lemma, since $\gcd(a, b) = 1$, $\exists x, y \in \mathbb{Z}$ with $ax + by = 1$. Let $\frac{1}{b} \in \mathbb{Z}[\frac{1}{b}]$, then
     $$\frac{1}{b} = \frac{(ax + by)}{b} = \frac{a}{b}x + y \in \mathbb{Z}[\frac{a}{b}]$$
   - **Claim:** $\mathbb{Z}[\frac{1}{b}] \supseteq \mathbb{Z}[\frac{a}{b}]$
     Let $\frac{a}{b} \in \mathbb{Z}[\frac{a}{b}]$ then
     $$\frac{a}{b} = a\frac{1}{b} \in \mathbb{Z}[\frac{1}{b}]$$

   So $\mathbb{Z}[\frac{1}{b}] = \mathbb{Z}[\frac{a}{b}]$. ☐

   (b). *Proof.* Let $A \subseteq \mathbb{Q}$ be a subring of $\mathbb{Q}$ such that $1 \in A$. Recall intermediate rings
   $$\mathbb{Z} \subseteq A \subseteq \mathbb{Q}$$
   Are identified with localizations of $\mathbb{Z}$. Prime ideals of $\mathbb{Z}$ are exactly $p\mathbb{Z}$ for $p \in \mathbb{Z}$ prime. For each ideal $P = p\mathbb{Z}$, the localization $P^{-1}\mathbb{Z}$ is isomorphic to $\mathbb{Z}[\frac{1}{p}]$ (by the universal property). So let $A = P^{-1}\mathbb{Z} \cong \mathbb{Z}[\frac{1}{p}]$ be some localization. By proposition 6.17, $\mathbb{Z}$ Noetherian implies $P^{-1}\mathbb{Z} \cong \mathbb{Z}[\frac{1}{p}]$ Noetherian. Therefore A is Noetherian. ☐

9. Let $p \in \mathbb{Z}$ be prime, and let $A := \mathbb{Z}_{(p)}$. Show that the ideal $(px - 1)$ is maximal in $A[x]$, and has height 1. Show that (p, x) is maximal in $A[x]$ and has height 2.

   Proof. Note that $\mathbb{Z}$ has dimension 1 (it is Noetherian), and localizations of Noetherian domains are themselves Noetherian, so $\dim(A) = 1$. Then, $\dim(A[x]) = 1 + 1 = 2$. So every maximal ideal has height at most 2.

- Consider the quotient ring

$$A[x]/(px-1)$$

This sets $px = 1 \implies x = \frac{1}{p} \in A[x]/(px-1)$ there are no polynomials (they have degree at most 0). And, by localization at (p), every nonzero $a \in A-(p)$ is a unit, and by setting $x = \frac{1}{p}$, every nonzero $q \in (p)$ is a unit. Therefore all nonzero elements are units, so $A[x]/(px-1) \cong \mathbb{Q}$ is a field, so $(px-1)$ is maximal in $A[x]$. The only possible prime ideal between (0) and $(px-1)$ is a degree 0 polynomial, i.e. a constant. By locality of A, (p) is its unique prime ideal, so we check if $(p) \subseteq (px-1)$. Assume

$$p \in (px-1) \implies p = a(px-1)$$

But LHS is degree 0 and RHS has degree at least 1. So $(p) \not\subset (px-1)$, then the chain $(0) \subset (px-1)$ gives $\mathrm{ht}((px-1)) = 1$.

- Consider the quotient ring

$$A[x]/(p,x) \cong (A[x]/(p))/(x) \cong A/(p)[x]/(x) \cong \mathbb{Q}$$

Because $A/(p) \cong \mathbb{Q}$ as A is a local Noetherian domain with maximal ideal (p), and $Q[x]/(x) \cong \mathbb{Q}$. So (p,x) is maximal in $A[x]$. It has a chain

$$(0) \subset (p) \subset (p,x)$$

Because $(p) \subset (p,x)$ by definition, so (p,x) has height 2.

□

10. Describe $\mathrm{Spec}(\mathbb{Z}[x])$.

For all prime p, $(p) \in \mathrm{Spec}(\mathbb{Z})$ so $(p) \in \mathrm{Spec}(\mathbb{Z}[x])$. By problem 1.5, for any irreducible polynomial $\bar{g}(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$, we have $(p, g(x)) \in \mathrm{Spec}(\mathbb{Z}[x])$, where $g(x)$ is the preimage of $\bar{g}(x)$ under the natural reduction map. As described in the previous problem, all ideals of $\mathbb{Z}[x]$ have height 1 or 2, so this is every prime ideal of $\mathbb{Z}[x]$.

11. Let A be a commutative ring. Let I be any subset of A. Let $V(I) := \{P \in \mathrm{Spec}(A) \mid I \subseteq P\}$. Now let I_1 and I_2 be two ideals of A.

(a). Show that $V(I_1 \cap I_2) = V(I_1 I_2) = V(I_1) \cup V(I_2)$.

(b). Show that $V(I_1 + I_2) = V(I_1) \cap V(I_2)$.

(c). Show that the sets $V(I)$, I an ideal in A, satisfy the axioms for closed sets in a topological space. The resulting topology on $\mathrm{Spec}(A)$ is called the *Zariski topology*.

Proof. (a). Let $P \in V(I_1 I_2)$. Then $I_1 I_2 \subseteq P$, but $P \in \mathrm{Spec}(A)$ so either $I_1 \subseteq P$ or $I_2 \subseteq P$. So

$$V(I_1 I_2) = V(I_1) \cup V(I_2)$$

We always have $I_1 I_2 \subseteq I_1 \cap I_2$.So

$$V(I_1 \cap I_2) \subseteq V(I_1 I_2)$$

But if P is a prime ideal containing I_1, it also contains all subsets of I_1, so it must contain $I_1 \cap I_2 \subseteq I_1$. Similarly if P contains I_2, it must also contain the intersection. So we have

$$V(I_1 I_2) \subseteq V(I_1 \cap I_2)$$

So

$$V(I_1 I_2) = V(I_1 \cap I_2)$$

Combining, we get

$$V(I_1 \cap I_2) = V(I_1 I_2) = V(I_1) \cup V(I_2)$$

(b). Let $P \in V(I_1 + I_2)$. So $I_1 + I_2 = \{a + b \mid a \in I_1, b \in I_2\} \subseteq P$. So clearly $I_1 \subseteq P$ and $I_2 \subseteq P$. Then

$$V(I_1 + I_2) \subseteq V(I_1) \cap V(I_2)$$

Let $P \in V(I_1) \cap V(I_2)$, then both I_1 and I_2 are subsets of P, and so $I_1 + I_2 \subseteq P$. So

$$V(I_1) \cap V(I_2) \subseteq V(I_1 + I_2)$$

Combining,

$$V(I_1 + I_2) = V(I_1) \cap V(I_2)$$

(c). Let $V(I)$ for I an ideal be a closed set. Then we have shown:

i. Finite union,

$$V(I_1) \cup V(I_2) = V(I_1 I_2)$$

is a closed set.

ii. Finite intersection

$$V(I_1) \cap V(I_2) = V(I_1 + I_2)$$

is a closed set.

iii. Finally, consider the ideals (0) and A, clearly,

$$V((0)) = \mathrm{Spec}(A)$$

as $(0) \subseteq P$ for all prime ideals P. Similarly,

$$V(A) = \emptyset$$

Because no prime ideal contains all of A. So the empty set and the whole space are closed sets.

So the sets $V(I)$ form a topology on $\mathrm{Spec}(A)$.

□

12. Let $\psi : A \to B$ be a ring homomorphism. Endow $\mathrm{Spec}(B)$ and $\mathrm{Spec}(A)$ with the Zariski topology. Show that $\mathrm{Spec}(\psi)$ is a continuous map. Spec is a contravariant functor from the category of commutative rings to the category of topological spaces.

Proof. Let $\psi : A \to B$ be a ring homomorphism and endow $\mathrm{Spec}(B)$ and $\mathrm{Spec}(A)$ with the Zariski topology. Let $J \subset B$ be an ideal. Then $V(J) \subset \mathrm{Spec}(B)$ is a closed set. We must show that

$$\mathrm{Spec}(\psi)^{-1}(V(J)) \subset \mathrm{Spec}(A)$$

is closed. By definition, $V(J) = \{P \in \mathrm{Spec}(B) \mid J \subseteq P\}$. Then,

$$\mathrm{Spec}(\psi)^{-1}(V(J)) = \{Q \in \mathrm{Spec}(A) \mid \psi(Q) \in V(J)\}$$

And $\psi(Q) \in V(J) \implies \psi(Q) \subseteq J$. So

$$\mathrm{Spec}(\psi)^{-1}(V(J)) = \{Q \in \mathrm{Spec}(A) \mid \psi(Q) \subseteq J\} = V(\psi^{-1}(J))$$

Is the set of prime ideals $Q \in \mathrm{Spec}(A)$ which contain the preimage $\psi^{-1}(J)$. By definition of the Zariski topology, $V(\psi^{-1}(J))$ is closed, so $\mathrm{Spec}(\psi)$ is a continuous map. □