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 $q \neq 1$. $\square$

   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! □

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

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

Proof. □

(c).

8. (a). Let k be any field. Let $A \coloneqq k[x_1, \dots, x_n, \dots]$ 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. □

(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) □

9. Let k be a field, and $A := k[x_1, \ldots, x_n]$. Let $\bar{k}$ denote an algebraic closure of k, and let $B := \bar{k}[x_1, \ldots, x_n]$. 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

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

   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 $P(x_1, \ldots, x_n)$ 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 $\{m_1, \ldots, m_n\}$ 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 $\{m_1, \ldots, m_n\}$ with coefficients from $\mathcal{M}$ and with coefficients from A:

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

Since $\{m_1, \ldots, m_n\}$ is a basis, we have either $(a_i - \mu_i) = 0$ or $m_i = 0$ for all $i \in \{1, \ldots, n\}$. 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 $\operatorname{rank}_A(M)$, is the dimension of the K-vector space $M_{(0)}$.

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

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

Proof. (a). ($\Longrightarrow$) 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.

(b).

$\square$