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: Due to a theorem (not in the book :/), the ring $\mathbb{Z}[x]$ is finitely generated iff x is algebraic over $\mathbb{Z}$. We have

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

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 $\mathbb{Z}[x]$
   (Because modding by it gave a field.) □

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 $A \coloneqq k[x_1, \dots, x_n, \dots]$ 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. $\square$

(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) □

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 $k[x_1, \ldots, x_n]$). So, choose an arbitrary element $\alpha \in B$. There are two cases:

   (a) If $\alpha \in A$, then we are done because $x_i - \alpha$ is a polynomial with coefficients in A 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.

   □