

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

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

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

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 $\mathbb{Z}[x] \rightarrow (\mathbb{Z}/p\mathbb{Z})[x]$ 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

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

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.) \square

6. Show that a principal 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 $(a) \subset A$, 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

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

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

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

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

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

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