

Problem 1 (7.6). 1. Let F be a non-trivial field and $F[[x]]$ the set of all formal power series

$$f(x) = \sum_{n=0}^{\infty} a_n x^n$$

where $a_i \in F$. Prove that $F[[x]]$ is an integral domain under the following addition and multiplication:

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

and

$$\left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} \left(\sum_{i+j=n} a_i b_j \right) x^n$$

Prove that $f(x)$ is a unit if and only if the constant term of $f(x)$ is non-zero.

2. Let R be a ring and S a subring of R . Prove that $M_n(S)$ is a subring of $M_n(R)$ for any integer $n \geq 1$.
3. Let R be a commutative ring and G a finite group.
 - (a) Prove that g is a unit of $R[G]$ for any $g \in G$.
 - (b) Prove or disprove that $G = R[G]^X$.
 - (c) If S is a subring of R , then $S[G]$ is a subring of $R[G]$.
4. Let R be a commutative ring and G be a finite group
 - (a) Let $\Lambda = \sum_{g \in G} g$. Prove that Λ is in the center of $R[G]$.
 - (b) Let K be a conjugacy class in G . Prove that $k = \sum_{g \in K} g$ is in the center of $R[G]$.
 - (c) Let K_1, \dots, K_r be the conjugacy classes of G and $k_i = \sum_{g \in K_i} g$ for $i = 1, \dots, r$. Prove that x is in the center of $R[G]$ if, and only if, $x = \sum_{i=1}^r a_i k_i$ for some $a_i \in R$.

Proof. 1. In order to show that $F[[x]]$ is an integral domain we must show that addition is associative, commutative, has identity, and has inverse. That multiplication is associative, commutative, has identity, and that it distributes over addition. For each of the following statements consider $\sum_{n=0}^{\infty} a_n, \sum_{n=0}^{\infty} b_n, \sum_{n=0}^{\infty} c_n \in F[[x]]$.

- For additive identity we let all terms be 0. Then

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} 0 x^n = \sum_{n=0}^{\infty} (a_n + 0) x^n = \sum_{n=0}^{\infty} 0 x^n + \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} a_n x^n$$

- For additive associativity we have

$$\begin{aligned} \left(\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n \right) \sum_{n=0}^{\infty} c_n x^n &= \sum_{n=0}^{\infty} ((a_n + b_n) + c_n) x^n = \sum_{n=0}^{\infty} (a_n + (b_n + c_n)) x^n \\ &= \sum_{n=0}^{\infty} a_n x^n + \left(\sum_{n=0}^{\infty} b_n x^n + \sum_{n=0}^{\infty} c_n x^n \right) \end{aligned}$$

- For additive commutativity we have

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n = \sum_{n=0}^{\infty} (b_n + a_n) x^n = \sum_{n=0}^{\infty} b_n x^n + \sum_{n=0}^{\infty} a_n x^n$$

- For additive inverse we have

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} (-a_n) x^n = \sum_{n=0}^{\infty} (a_n - a_n) x^n = \sum_{n=0}^{\infty} 0 x^n$$

- For multiplicative identity let $b_0 = 1$ and $b_n = 0$ for $n > 0$. Then

$$\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} \left(\sum_{i+j=n} a_i b_j \right) x^n$$

However since $b_n = 0$ for $n > 0$ the only non-zero term in the inner sum will be when $i = n$ and $j = 0$. Thus

$$\sum_{n=0}^{\infty} \left(\sum_{i+j=n} a_i b_j \right) x^n = \sum_{n=0}^{\infty} a_n x^n$$

- For associativity of multiplication we have

$$\begin{aligned} \left(\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n \right) \cdot \sum_{n=0}^{\infty} c_n x^n &= \left(\sum_{n=0}^{\infty} \left(\sum_{i+j=n} a_i b_j \right) x^n \right) \cdot \sum_{n=0}^{\infty} c_n x^n \\ &= \sum_{n=0}^{\infty} \left(\sum_{i+j=n} \left(\sum_{h+k=i} a_h b_k \right) c_j \right) x^n \\ &= \sum_{n=0}^{\infty} \left(\sum_{i+j=n} a_i \left(\sum_{j+k=j} b_h c_k \right) \right) x^n = \sum_{n=0}^{\infty} a_n x^n \cdot \left(\sum_{n=0}^{\infty} b_n x^n \cdot \sum_{n=0}^{\infty} c_n x^n \right) \end{aligned}$$

- For commutativity of multiplication we have

$$\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} \left(\sum_{i+j=n} a_i b_j \right) x^n = \sum_{n=0}^{\infty} \left(\sum_{i+j=n} b_i a_j \right) x^n = \sum_{n=0}^{\infty} b_n x^n \cdot \sum_{n=0}^{\infty} a_n x^n$$

- For distributivity we have

$$\begin{aligned} \sum_{n=0}^{\infty} c_n x^n \left(\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n \right) &= \sum_{n=0}^{\infty} c_n x^n \cdot \sum_{n=0}^{\infty} (a_n + b_n) x^n \\ &= \sum_{n=0}^{\infty} \left(\sum_{i+j=n} c_i (a_j + b_j) \right) x^n = \sum_{n=0}^{\infty} \left(\sum_{i+j=n} c_i a_j + c_i b_j \right) x^n \\ &= \sum_{n=0}^{\infty} \left(\sum_{i+j=n} c_i a_j + \sum_{i+j=n} c_i b_j \right) x^n = \sum_{n=0}^{\infty} \left(\sum_{i+j=n} c_i a_j \right) x^n + \sum_{n=0}^{\infty} \left(\sum_{i+j=n} c_i b_j \right) x^n \\ &= \sum_{n=0}^{\infty} c_n x^n \cdot \sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} c_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n \end{aligned}$$

To show that $F[[x]]$ is an integral domain we must show that $F[[x]]$ has no zero-divisors. Suppose that $\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n = 0$. Without loss of generality assume that both a_0 and b_0 are not 0. If the first k terms consisted of only zeros we could factor out x^k and proceed with this assumption. Then the zero term would be $\sum_{i+j=0} a_i b_j = a_0 b_0 = 0$. Since F is a field either a_0 or b_0 are 0. Without loss of generality assume that it's b_0 . We then proceed by induction. Assume that $b_k = 0$ for $k \leq m$. Then consider the term b_{m+1} . The sum for the $m+1$ coefficient is $\sum_{i+j=m+1} a_i b_j$. However by our inductive hypothesis $b_k = 0$ for $k \leq m$. Which leaves us with $a_0 b_{m+1} = 0$. However we already assumed that $a_0 \neq 0$ which implies that $b_{m+1} = 0$.

Therefore, by induction, all terms of $\sum_{n=0}^{\infty} b_n x^n$ are zero. As such the only way that $\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n = 0$ can hold is if one of the series is zero.

Therefore since $F[[x]]$ is a commutative ring with no zero divisors it is an integral domain.

Now we will show that a series $\sum_{n=0}^{\infty} a_n x^n$ is a unit if and only if $a_0 \neq 0$. First suppose that $\sum_{n=0}^{\infty} a_n x^n$ is a unit. Then there is a series such that $\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n = 1$. However this implies that $a_0 b_0 = 1$ and the only way this can occur is if a_0 is also a unit in F . However since F is a field this will hold so long as $a_0 \neq 0$.

Now suppose that $\sum_{n=0}^{\infty} a_n x^n$ is a series such that $a_0 \neq 0$. Then define $b_0 = a_0^{-1}$ and $b_n = a_0^{-1}(-\sum_{i+j=n-1} a_i b_j)$ for $n > 0$. This will cause the sum $\sum_{i+j=n} a_i b_j = 0$ for all $n > 0$. Thus

$$\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} \left(\sum_{i+j=n} a_i b_j \right) x^n = 1$$

Therefore $f \in F[[x]]$ is a unit if and only if the constant term is nonzero.

2. Let S be a subring of R . Then consider the matrices $A, B \in M_n(S)$. Let A_{ij} denote the ij th entry in the matrix.

For $A+B$ we have $(A+B)_{ij} = A_{ij} + B_{ij} \in S$ since S is a subring. Since this hold for all entries we have that $A+B \in M_n(S)$.

For AB we have $(AB)_{ij} = \sum_{k=1}^n A_{ik} B_{kj}$. However each $A_{ik}, B_{kj} \in S$ since S is a subring which implies that $(AB)_{ij} \in S$ and therefore $AB \in M_n(S)$. Since $M_n(S)$ is closed under multiplication and addition it is a subring of $M_n(R)$.

3. (a) Let $g \in G$. Then it has an inverse $g^{-1} \in G$ for which both $g, g^{-1} \in R[G]$. Thus we have $gg^{-1} = e = 1 \in R[G]$ which shows that g is a unit of $R[G]$.
(b) Let R be a ring with a non-trivial unit $r \in R$. Then $rg \cdot r^{-1}g^{-1} = 1e$ which implies that $rg \notin G$ but that $rg \in R[G]^X$. Therefore G may not equal $R[G]^X$.
(c) Let S be a subring of R and let $f := \sum_{g \in G} a_g g, g := \sum_{g \in G} b_g g \in S[G]$.
For $f+g$ we have $f+g = \sum_{g \in G} (a_g + b_g)g$ and since $a_g + b_g \in S$ due to S being a subring $f+g \in S[G]$.
For fg we have $fg = \sum_{k \in G} \left(\sum_{gh=k} a_g b_h \right) k$. However since S is a subring $\sum_{gh=k} (a_g b_h) \in S$ as it is a sum of terms in S . It then follows that $fg \in S[G]$.
Therefore if S is a subring of R then $S[G]$ is a subring of $R[G]$.
4. (a) Let $\sum_{g \in G} a_g g \in R[G]$. Then

$$\sum_{g \in G} a_g g \cdot \sum_{g \in G} g = \sum_{k \in G} \left(\sum_{gh=k} a_g \right) k$$

Since rings are associative under addition we have

$$\sum_{k \in G} \left(\sum_{gh=k} a_g \right) k = \sum_{k \in G} \left(\sum_{gh=k} a_h \right) k = \sum_{g \in G} g \cdot \sum_{g \in G} a_g g \sum$$

Therefore Λ is in the center of $R[G]$.

(b)

(c)

□

Problem 2 (7.7). For any nonzero integers a, b , prove that $(a, b) = (\gcd(a, b))$, $(a) \cap (b) = (\text{lcm}(a, b))$ and that $(a)(b) = (ab)$.

Proof.

□

Problem 3 (7.8). Let G be a finite group and R a commutative ring. Show that the map $\epsilon : R[G] \rightarrow R$ given by

$$\epsilon \left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} a_g$$

is a surjective ring homomorphism and $\ker \epsilon$ is the ideal generated by the set $\{g - e | g \in G\}$.

Proof.

□

Problem 4 (7.10). 1. Prove that $x^2 = 0$ or 1 for all $x \in \mathbb{Z}_4$

2. Prove that the equation $x^2 + y^2 = 3z^2$ has no nontrivial integer solution.

Proof. 1. For each case we have

- $0^2 \equiv 0 \pmod{4}$
- $1^2 \equiv 1 \pmod{4}$
- $2^2 \equiv 0 \pmod{4}$
- $3^2 \equiv 1 \pmod{4}$

Therefore the polynomial $x^2 = 0$ or 1 for all $x \in \mathbb{Z}_4$.

2.

□

Problem 5 (7.11). Let D be a square-free integer and I the ideal $(x^2 - D)$ of $\mathbb{Q}[x]$. Prove that

$$\mathbb{Q}[x]/I \cong \mathbb{Q}(\sqrt{D})$$

as rings. Find all the ideals of $\mathbb{Q}[x]$ containing I .

Proof.

□