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 $K_1, \ldots, K_r$ be the conjugacy classes of G and $k_i = \sum_{g \in K_i} g$ for $i = 1, \ldots, r$. 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

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

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

- 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

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

- 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

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

- For associativity of multiplication we have

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

$$= \sum_{n=0}^{\infty} \left(\sum_{i+j=n} \left(\sum_{h+k=i} a_h b_k \right) c_j \right) x^n$$

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

- 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

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

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

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

$$= \sum_{n=0}^{\infty} c^n x^n \cdot \sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} c_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n$$

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 from each term. It would then reduce to multiplying two series 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 ijth 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) Let $\sum_{g\in G} a_g g \in R[G]$. Then

$$\sum_{g\in G} a_g g\cdot\sum_{g\in K} g = \sum_{g\in G}\left(\sum_{hk=g} a_h b_k\right) g$$

where $b_k = 0$ if $k \notin K$ and 1 if $b_k \in K$. Since K is a conjugacy class we have that $gkg^{-1} = k' \in K$. It then follows that $gk = k'g$ for some k'. Thus we can rewrite the above equation as

$$\sum_{g\in G}\left(\sum_{hk=g} a_h b_k\right) g = \sum_{g\in G}\left(\sum_{hk=g} b_{k'} a_h\right) g = \sum_{g\in K} g\cdot\sum_{g\in G} a_g g$$

Which completes the proof.

(c) Let $x = \sum_1^r a_i k_i$. Since $Z(R[G])$ is a subring of $R[G]$ it then follows that $x \in Z(R[G])$. Next suppose that $x \in Z$ and let $a = \sum_{g\in G} a_g g \in R[G]$. Since $xa = ax$ it follows that $\sum_{hk=g} x_h a_k = \sum_{hk=g} a_h x_k$ for all $g \in G$. Now suppose that x was not a linear combination of k_is. Then there would be a K_i for which there would be $k, k' \in K_i$ such that $x_k \neq x_{k'}$. Since k, k' are in the same conjugacy class it follows that there exists a $g \in G$ such that $gk = k'g$. However this means that

$$\sum_{hf=g} a_h x_f \neq \sum_{hf=g} x_h x_f$$

since when we switch sides we will swap out x_k for $x_{k'}$ making the sums inequal which is a contradiction.

Therefore $x \in Z(R[G])$ is and only if $x = \sum_1^r a_i k_i$.

□

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

Proof.

- Let $na + mb \in (a, b)$. There exist $\alpha, \beta \in \mathbb{Z}$ such that $\alpha \gcd(a, b) = a$ and $\beta \gcd(a, b) = b$. Then $na + mb = n\alpha \gcd(a, b) + m\beta \gcd(a, b) \in (\gcd(a, b))$ which implies that $(a, b) \subset (\gcd(a, b))$.

  Now let $n \gcd(a, b) \in (\gcd(a, b))$. Then there exist $\alpha, \beta \in \mathbb{Z}$ such that $\alpha a + \beta b = \gcd(a, b)$. Thus $n \gcd(a, b) = n\alpha a + n\beta b \in (a, b)$ implying that $(\gcd(a, b)) \subset (a, b)$.

  Therefore $(a, b) = (\gcd(a, b))$.

- Let $d = \mathrm{lcm}(a, b)$. Then there exists $\alpha, \beta \in \mathbb{Z}$ such that $\alpha a = \beta b = d$. Then if $nd \in (d)$ we have $nd = n\alpha a = n\beta b$ which implies that $nd \in (a) \cap (b)$.

  Let $f \in (a) \cap (b)$. Then there exist $\alpha, \beta \in \mathbb{Z}$ such that $\alpha a = \beta b = f$. However this implies that both a and b divide f and as such d divides f and there exists a $\delta \in \mathbb{Z}$ such that $\delta d = f$. It then follows that $f \in (d)$.

  Therefore $(a) \cap (b) = (\mathrm{lcm}(a, b))$.

- Let $nab \in (ab)$. Then $na \cdot 1b \in (a)(b)$.

  Otherwise let $na \cdot mb \in (a)(b)$. Then $namb = (nm)(ab) \in (ab)$.

  Therefore $(a)(b) = (ab)$.

□

Problem 3 (7.8)**.** *Let G be a finite group and R a commutative ring. Show that the map $\epsilon : R[G] \to R$ 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. First we'll show that it preserves addition. Let $\sum_{g\in G} a_g g, \sum_{g\in G} b_g g \in R[G]$. Then

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

For multiplication we have

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

$$= \sum_{g\in G}\left(\sum_{hk=g} a_h b_k\right) = \epsilon\left(\sum_{g\in G}\left(\sum_{hk=g} a_h b_k\right) g\right) = \epsilon\left(\sum_{g\in G} a_g g \cdot \sum_{g\in G} b_g g\right)$$

Therefore ϵ is a ring homomorphism.

Let $a \in R$. Then $\epsilon(ag) = a$. Therefore the map ϵ is surjective.

Now suppose that $\sum_{g\in G} a_g g \in \ker\epsilon$. Then $\sum_{g\in G} a_g = 0$. It then follows that $\sum_{g\in G\setminus\{e\}} a_g + a_e = 0$. Which implies that $a_e = -\sum_{g\in G\setminus\{e\}} a_g$. This implies that we can rewrite our original term as $\sum_{g\in G} a_g(g - e)$ which shows that $\ker\epsilon \subset \langle\{g - e|g \in G\}\rangle$.

Now suppose that we have $\sum_{g\in G} a_g(g - e) = \sum_{g\in G} a_g g - \sum_{g\in G} a_g$. Then

$$\epsilon\left(\sum_{g\in G} a_g g - \sum_{g\in G} a_g\right) = \sum_{g\in G} a_g - \sum_{g\in G} a_g = 0$$

Therefore the kernel of ϵ is the set generated by $\{g - e|g \in G\}$. □

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

- $0^2 \equiv 0 \mod 4$
- $1^2 \equiv 1 \mod 4$

- $2^2 \equiv 0 \mod 4$
- $3^2 \equiv 1 \mod 4$

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

2. First we will verify that $x^2 + y^2 = 3z^2$ has no non-trivial solutions in $\mathbb{Z}_3$. There scenarios are:

   - If $x = y = 1$ then $1 + 1 = 2$.
   - If $x = 0$, $y = 1$ then $0 + 1 = 1$.
   - If $x = 1$, $y = 0$ then $1 + 0 = 1$.

   Therefore there are no non-trivial solutions of $x^2 + y^2 = 3z^2$.

   Thus if a non-trivial integer solution does exist it must be that $x = 3k$ and $y = 3j$. Then the equation shifts to $9k^2 + 9j^2 = 3z^2$ which then gives us $3(k^2 + j^2) = z^2$. This implies that $z = 3h$. Rewrite again once more and we get $k^2 + j^2 = 3h^2$. However this is the original equation which implies that we can factor out an arbitrary number of 3s from x, y, z. Therefore the only solution where $x, y|3$ is the trivial solution.

   Therefore $x^2 + y^2 = 3z^2$ has no non-trivial integer solutions.

□

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. First we show that $\mathbb{Q}[x]/I \cong \mathbb{Q}(\sqrt{D})$. Define $\varphi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{D}]$ as $\varphi(f(x)) = f(\sqrt{D})$. If $f(x) = \sum_0^n r_i x^i$ then $\varphi(f(x)) = \sum_0^n r_i \sqrt{D}^i \in \mathbb{Q}[\sqrt{D}]$. To show that it is a homomorphism first consider addition for $f, g \in \mathbb{Q}[x]$. Then

$$\varphi(f+g) = \varphi(\sum_0^n (r_i + s_i)x^i) = \sum_0^n (r_i + s_i)D^{i/2} = \sum_0^n r_i D^{i/2} + \sum_0^n s_i D^{i/2} = \varphi(f) + \varphi(g)$$

For multiplication we have

$$\varphi(fg) = \varphi(\sum_0^n \left(\sum_{i+j=n} r_i s_j \right) x^i) = \sum_0^n \left(\sum_{i+j=n} r_i s_j \right) D^{i/2} = \left(\sum_0^n r_i D^{i/2} \right) \left(\sum_0^n s_i D^{i/2} \right) = \varphi(f)\varphi(g)$$

To show that it is surjective consider $a + b\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$. Then $\varphi(a + bx) = a + b\sqrt{D}$ which shows that φ is a surjection.

The kernel of φ is the ideal $\langle (x^2 - D) \rangle$. To see this let $f \in \langle (x^2 - D) \rangle$. Then $f = g(x^2 - D)$ which implies that

$$\varphi(f) = \varphi(g)\varphi(x^2 - D) = \varphi(g)0 = 0$$

Therefore $\langle (x^2 - D) \rangle \subset \ker \varphi$. Now let $f \in \ker \varphi$. This implies that $f(\sqrt{D}) = 0$. However this also implies that $f(-\sqrt{D}) = 0$. It then follows that $f = g(x^2 - D)$ for some g and as such $f \in \langle (x^2 - D) \rangle$. Therefore the kernel of φ is the ideal $\langle (x^2 - D) \rangle$.

Therefore by the first isomorphism theorem of rings we have that $\mathbb{Q}[x]/I \cong \mathbb{Q}(\sqrt{D})$.

The ideals that contain $\langle (x^2 - D) \rangle$ will be those generated by the polynomials f where there exists a g such that $fg = (x^2 - D)$. In this case the polynomials where this holds are $1, (x - \sqrt{D}), (x + \sqrt{D}), (x^2 - D)$. However since D is square-free the middle two do not exist inside $\mathbb{Q}[x]$ and as such the only ideals containing $\langle (x^2 - D) \rangle$ are itself and the whole ring. □