23.21.1 Prove if R is a domain so is the ring of formal power series $R[[t]]$.

Solution Suppose otherwise, and let

$$f(t) = \sum_{i=0}^{\infty} a_i t^i,\ g(t) = \sum_{i=0}^{\infty} b_i t^i \in R[[t]]$$

be non-zero with $f(t) \cdot g(t) \equiv 0$. Let a_n and b_m be the first non-zero coefficients so that

$$f(t) = \sum_{i=0}^{\infty} a_{i+n} t^{i+n} \quad \text{and} \quad g(t) = \sum_{i=0}^{\infty} b_{i+m} t^{i+m}.$$

Then

$$0 = f(t) \cdot g(t) = \sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} a_{k+n} b_{i-k+m} \right) t^i \implies \sum_{k=0}^{i} a_{k+n} b_{i-k+m} = 0\ \forall i.$$

In particular, if $i = 0$, we see that $a_n b_m = 0$. Since R is a domain, this implies that $a_n = 0$ or $b_m = 0$, but this is a contradiction since we assumed that they were both non-zero. Thus, either $f(t)$ or $g(t)$ has no first non-zero coefficient, i.e., one of them is 0, so $R[[t]]$ is a domain.

23.21.2 Let R be a commutative ring. Show that if $f = 1 + \sum_{i=1}^{\infty} a_i$ is a formal power series in $R[[t]]$, then one can determine $b_1, \ldots, b_n, \ldots$ such that $g = 1 + \sum_{i=1}^{\infty} b_i$ is the multiplicative inverse of f in $R[[t]]$. In particular,

$$R[[t]]^\times = \left\{ a_0 + \sum_{i=1}^{\infty} a_i \in R[[t]] \mid a_0 \in R^\times \right\}.$$

Solution Let f be as in the problem. We wish to determine g so that

$$1 = f(t) \cdot g(t) = \sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} a_k b_{i-k} \right) t^i = 1 + \sum_{i=1}^{\infty} \left(\sum_{k=0}^{i} a_k b_{i-k} \right) t^i.$$

For all $i \geq 1$, we want

$$0 = \sum_{k=0}^{i} a_k b_{i-k} = b_i + \sum_{k=1}^{i} a_k b_{i-k} \implies b_i = -\sum_{k=1}^{i} a_k b_{i-k}.$$

Thus, if we have $b_0, b_1, \ldots, b_{i-1}$, then we can calculate b_i for any i, by induction. We can calculate b_1, since we know that $b_0 = 1$, so the base case holds, which shows that we can determine such a g.

We'll now show that the given sets in the problem are equal.

"$\subseteq$"

Let $f(t) \in R[[t]]^\times$, and write

$$f(t) = a_0 + \sum_{i=1}^{\infty} a_i.$$

By definition, $f(t)$ is a unit, so there exists $g(t) \in R[[t]]$ so that $f(t) \cdot g(t) = 1$. If b_0 is the first coefficient of $g(t)$, then we see that $a_0 b_0 = 1$, by definition of multiplication. This shows that a_0 is a unit, which shows the first direction.

"$\supseteq$"

$$f(t) \in \left\{ a_0 + \sum_{i=1}^{\infty} a_i \in R[[t]] \mid a_0 \in R^\times \right\},$$

there exists $a \in R$ so that $a_0 a = 1$, by definition, so that

$$af(t) = 1 + \sum_{i=1}^{\infty} aa_0.$$

By the first part of this problem, there exists $g(t)$ so that $af(t) \cdot g(t) = 1$. Since R is commutative, $af(t) \cdot g(t) = f(t) \cdot ag(t) = 1$, so $f(t)$ is a unit, which shows this direction.

Hence,

$$R[[t]]^\times = \left\{ a_0 + \sum_{i=1}^{\infty} a_i \in R[[t]] \mid a_0 \in R^\times \right\}.$$

23.21.6 Show that a ring homomorphism $\varphi \colon R \to S$ is a monomorphism if and only if given any ring homomorphism $\psi_1, \psi_2 \colon T \to R$ with compositions satisfying $\varphi \circ \psi_1 = \varphi \circ \psi_2$, then $\psi_1 = \psi_2$.

Solution "$\implies$"

This direction is clear since $\varphi(x) = \varphi(y) \implies x = y$, for any $x, y \in R$.

"$\impliedby$"

Suppose that φ is non-injective. Then there exist $a \neq b \in R$ with $\varphi(a) = \varphi(b)$.

Define $\psi_1, \psi_2 \colon \mathbb{Z}[x] \to R$ by $\psi_1(x) = a$ and $\psi_2(x) = b$. It is clear where the rest of the elements of $\mathbb{Z}[x]$ are mapped to based on this, (e.g, $\psi_1(x^2) = a^2$, etc.) and this clearly defines a ring homomorphism.

Then this is clearly a ring homomorphism and $\varphi \circ \psi_1 = \varphi \circ \psi_2$. By assumption, this implies that $\psi_1 = \psi_2$, but this is impossible since $a \neq b$. Hence, φ must be injective.

23.21.9 If R is a ring satisfying $x^2 = x$ for all x in R, then R is commutative.

Solution First notice that

$$(-x)^2 - x = (-x) \cdot (-x) + (-x) \cdot x = (-x) \cdot (-x + x) = 0 \implies x = (-x)^2,$$

but $(-x)^2 = -x$. This tells us that $-x = x$, for any $x \in R$.

Let $x, y \in R$. Then

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + y + xy + yx \implies xy = -yx = yx,$$

as desired.

23.21.10 If R is a rng satisfying $x^3 = x$ for all x in R, then R is commutative.

Solution First notice that for any $x \in R$,

$$2x = (2x)^3 = 8x^3 = 8x \implies 6x = 0.$$

Let $x, y \in R$. Then

$$\begin{aligned} x + y = (x+y)^3 &= x^3 + x^2y + xyx + xy^2 + yx^2 + yxy + y^2x + y^3 \\ x - y = (x-y)^3 &= x^3 - x^2y - xyx + xy^2 - yx^2 + yxy + y^2x - y^3 \\ \implies 2y &= 2x^2y + 2xyx + 2yx^2 + 2y^3 \\ \implies 0 &= 2x^2y + 2xyx + 2yx^2 \end{aligned}$$

Multiplying by x on the left and on the right, we get the expressions

$0 = 2x^3y + 2x^2yx + 2xyx^2 = 2xy + 2x^2yx + 2xyx^2$ and $0 = 2x^2yx + 2xyx^2 + 2yx^3 = 2x^2yx + 2xyx^2 + 2yx$,

and subtracting them yields

$$0 = 2(xy - yx).$$

Lastly, notice that

$$x^2 + x = (x^2 + x)^3 = x^6 + 3x^5 + 3x^4 + x^3 = 4x^2 + 4x,$$

so $3x^2 + 3x = 0$. In particular, replacing x with $x + y$, we get

$$0 = 3(x^2 + xy + yx + y^2 + 3x + 3y) = 3(xy + yx) + 3(x^2 + x) + 6x + 3(y^2 + y) + 6y = 3(xy + yx),$$

since $6x = 0$ for any x.

Subtracting $0 = 2(xy - yx)$ from $0 = 3(xy + yx)$, we get

$$xy + 5yx = 0.$$

Since $6x = 0 \implies 5x = -x$ for any x, we get

$$xy - yx = 0,$$

so R is commutative.

23.21.11 Let R be a commutative ring and $\mathfrak{A}$ be an ideal in R satisfying

$$\mathfrak{A} = \mathfrak{m}_1 \cdots \mathfrak{m}_r = \mathfrak{n}_1 \cdots \mathfrak{n}_s$$

with all the $\mathfrak{m}_i$ distinct maximal ideals and all the $\mathfrak{n}_j$ distinct maximal ideals. Show that $r = s$ and there exists a $\sigma \in S_r$ satisfying $\mathfrak{m}_i = \mathfrak{n}_{\sigma(i)}$ for all i.

Solution Let $\mathfrak{a}, \mathfrak{b}$ be ideals and $\mathfrak{p}$ be a prime ideal. We'll first show that if $\mathfrak{ab} \subseteq \mathfrak{p}$, then $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$.

Suppose $\mathfrak{a} \subsetneq \mathfrak{p}$ and $\mathfrak{b} \subsetneq \mathfrak{p}$. Then there exist $a \in \mathfrak{a} \setminus \mathfrak{p}$ and $b \in \mathfrak{b} \setminus \mathfrak{p}$. By assumption, $ab \in \mathfrak{p}$, but $\mathfrak{p}$ is prime, so $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, a contradiction. Hence, $\mathfrak{p}$ contains $\mathfrak{a}$ or $\mathfrak{b}$. By induction, it follows that if $\mathfrak{a}_1 \cdots \mathfrak{a}_n \subseteq \mathfrak{p}$, then at least one of the $\mathfrak{a}_i$'s is contained in $\mathfrak{p}$.

Also, for any two ideals $\mathfrak{a}$ and $\mathfrak{b}$, $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$, since ideals are closed under multiplication from R.

Since each $\mathfrak{m}_i$ and $\mathfrak{n}_j$ are maximal, they are also prime, so we can apply the lemma above. Thus, for any $1 \le j \le s$,

$$\mathfrak{m}_1 \cdots \mathfrak{m}_r \subseteq \mathfrak{n}_j.$$

By the lemma, there exists i so that $\mathfrak{m}_i \subseteq \mathfrak{n}_j$. Since $\mathfrak{m}_i$ is maximal, it follows that $\mathfrak{m}_i = \mathfrak{n}_j$. Since the ideals are distinct, we now have

$$\mathfrak{m}_1 \cdots \mathfrak{m}_{i-1}\mathfrak{m}_{i+1} \cdots \mathfrak{m}_r \subseteq \mathfrak{n}_1 \cdots \mathfrak{n}_{j-1}\mathfrak{n}_{j+1} \cdots \mathfrak{n}_r.$$

We can repeat the same argument until the process terminates in finitely many steps. Then it is clear that $r = s$ (or else there will be at least one $\mathfrak{m}_i$ or $\mathfrak{n}_j$ leftover) and that for each $\mathfrak{m}_i$, by assumption, there exists a unique $\mathfrak{n}_j$ so that $\mathfrak{m}_i = \mathfrak{n}_j$, i.e., there exists $\sigma \in S_r$ so that $\mathfrak{m}_i = \mathfrak{n}_{\sigma(i)}$ for each i.

23.21.12 Let R be a commutative ring and $\mathfrak{A}$ an ideal of R. Suppose that every element in $R \setminus \mathfrak{A}$ is a unit of R. Show that $\mathfrak{A}$ is a maximal ideal of R and that, moreover, it is the only maximal ideal of R.

Solution Suppose $\mathfrak{B}$ is an ideal containing $\mathfrak{A}$.

Suppose there exists $a \in \mathfrak{B} \setminus \mathfrak{A} \subseteq R \setminus \mathfrak{A}$. By assumption, a is a unit, so there exists $b \in R \setminus \mathfrak{A}$ so that $ab = 1$. Since $\mathfrak{B}$ is an ideal, $1 = ab \in \mathfrak{B}$, so $\mathfrak{B} = R$. This shows that $\mathfrak{A}$ is maximal.

Now let $\mathfrak{B}$ be another maximal ideal. There must be some $a \in \mathfrak{B} \setminus \mathfrak{A}$. Otherwise, $\mathfrak{A} \subsetneq \mathfrak{B}$, which means that $\mathfrak{A}$ is not maximal. But as we showed above, this implies that $\mathfrak{B} = R$, a contradiction. Hence, $\mathfrak{A}$ is the only maximal ideal of R.

23.21.13 Let R be the set of all continuous functions $f\colon [0,1] \to \mathbb{R}$. Then R is a commutative ring under $+$ and $\cdot$ of functions. Show that any maximal ideal of R has the form $\{f \in R \mid f(a) = 0\}$ for some fixed a in $[0,1]$.

Solution Let $F_a = \{f \in R \mid f(a) = 0\}$, and let G_a be an ideal containing F_a. Clearly F_a is an ideal since $0 + 0 = 0$ and $c \cdot 0 = 0$, for any c.

If there exists $g \in G_a \setminus F_a$, then $g(a) \neq 0$, by definition. But this means that $G_a = R$:

Clearly $G_a \subseteq R$. Given $f \in R$ with $f(a) \neq 0$ and notice that because G_a is an ideal and constant functions are continuous,

$$\frac{f(a)}{g(a)} g(x) \in G_a.$$

Since $F_a \subseteq G_a$,

$$f(x) - \frac{f(a)}{g(a)} g(x) \in G_a.$$

But this means

$$f(x) = \left(f(x) - \frac{f(a)}{g(a)} g(x) \right) + \frac{f(a)}{g(a)} g(x) \in G_a,$$

so $G_a = R$, which means that F_a is maximal.

Now let $\mathfrak{m}$ be a maximal ideal of R. Assume that $\mathfrak{m}$ is not in the form given, and that for all $x \in [0,1]$, there exists a function $f_x \in \mathfrak{m}$ such that $f_x(x) \neq 0$.

By continuity, for all $x \in [0,1]$, there exists $\delta_x > 0$ so that $f_x(y) \neq 0$ if $y \in B_{\delta_x}(x) = \{y \in [0,1] \mid |x - y| < \delta_x\}$. Thus, $\{B_{\delta_x}(x)\}_{x \in [0,1]}$ covers $[0,1]$. By compactness, there exist $x_1, \ldots, x_n \in [0,1]$ so that $B_{\delta_{x_1}}, \ldots, B_{\delta_{x_n}}$ cover $[0,1]$.

Since $\mathfrak{m}$ is an ideal,

$$0 < \sum_{i=1}^{n} [f_{x_i}(x)]^2 \in \mathfrak{m}.$$

But this function is a unit, and its inverse is its reciprocal. Thus, $1 \in \mathfrak{m}$, so $\mathfrak{m} = R$, a contradiction, so, there exists some point $a \in [0,1]$ so that all functions in $\mathfrak{m}$ vanish at a.

23.21.17 Let $\mathfrak{A}_1, \dots, \mathfrak{A}_n$ be ideals in R, at least $n-2$ of which are prime. Let $S \subseteq R$ be a subrng (it does not need to have a 1) contained in $\mathfrak{A}_1 \cup \cdots \cup \mathfrak{A}_n$. Then one of the $\mathfrak{A}_j$'s contains S. In particular, if $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are prime ideals in R and $\mathfrak{B}$ is an ideal properly contained in S satisfying $S \setminus \mathfrak{B} \subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$, then S lies in one of the $\mathfrak{p}_i$'s.

Solution We'll proceed by induction.

Base case: $n = 2$

Let $S \subseteq \mathfrak{A}_1 \cup \mathfrak{A}_2$. Assume that $S \subsetneq \mathfrak{A}_1$ and $S \subsetneq \mathfrak{A}_2$, so that there exist $x, y \in S$ with $x \in \mathfrak{A}_1 \setminus \mathfrak{A}_2$ and $y \in \mathfrak{A}_2 \setminus \mathfrak{A}_1$.

Since $x + y \in S$, we have $x + y \in \mathfrak{A}_1$ or $x + y \in \mathfrak{A}_2$. But this means that

$$y = (x + y) - x \in \mathfrak{A}_1 \quad \text{or} \quad x = (x + y) - y \in \mathfrak{A}_2,$$

which is a contradiction. Hence $S \subseteq \mathfrak{A}_1$ or $S \subseteq \mathfrak{A}_2$.

Inductive step:

Let $S \subseteq \mathfrak{A}_1 \cdots \mathfrak{A}_n$, and assume that $\mathfrak{A}_1, \dots, \mathfrak{A}_{n-2}$ are prime. Assume that S is not contained in any of them, so there exist x, y, and $1 \le i < j \le n$ so that $x \in \mathfrak{A}_i \setminus \mathfrak{A}_j$ and $y \in \mathfrak{A}_j \setminus \mathfrak{A}_i$.

Since $x + y \in S \subseteq \mathfrak{A}_1 \cup \cdots \cup \mathfrak{A}_n$, there exists $1 \le k \le n$ so that $x + y \in \mathfrak{A}_k$. Then $k \ne i$ or $k \ne j$. Otherwise, if $k = i$,

$$y = (x + y) - x \in \mathfrak{A}_i,$$

but we assumed that $y \notin \mathfrak{A}_i$. The same argument holds if $j = i$. Hence, we have

$$S \subseteq \mathfrak{A}_1 \cdots \mathfrak{A}_{i-1}\mathfrak{A}_{i+1} \cdots \mathfrak{A}_n \quad \text{or} \quad S \subseteq \mathfrak{A}_1 \cdots \mathfrak{A}_{j-1}\mathfrak{A}_{j+1} \cdots \mathfrak{A}_n.$$

In either case, we've reduced the problem to having $n - 1$ ideals, so by induction, $S \subseteq \mathfrak{A}_k$ for some $1 \le k \le n$, as desired.

---

1 Find a maximal ideal in $R = \mathbb{Z}[\sqrt{-5}]$ containing the principal ideal (3). Can you find another?

Solution We claim that (3) is a maximal ideal.

Let $a + b\sqrt{-5} \in \mathfrak{A} \supsetneq (3)$, i.e., at least one of a and b is not an integer multiple of 3. Without loss of generality, assume that this is a. Then because 3 is prime, $\gcd(3, a) = 1$, so there exist $x, y \in \mathbb{Z}$ so that $3x + ay = 1$. Since $3 \in \mathfrak{A}$, it follows that

$$1 + yb\sqrt{-5} \in \mathfrak{A}.$$

If b is divisible by 3, it follows that $1 \in \mathfrak{A}$, which implies that $\mathfrak{A} = R$.

On the other hand, if b is not divisible by 3, by the same argument as above, we can write $3c + ybd = 1$ and $-3c - ybd = -1$ to deduce that $1 + \sqrt{-5}, 1 - \sqrt{-5} \in \mathfrak{A}$. Hence, $2 \in \mathfrak{A}$, so since $3 \in \mathfrak{A}$, we have $3 - 2 = 1 \in \mathfrak{A}$, so $\mathfrak{A} = R$ in this case also.

Hence, $\mathfrak{A} = R$, so (3) is maximal.