.1 Unique factorization in polynomial rings

Problem .1.1. Prove Lemma 4.1.

Lemma 4.1. *Let R be a ring, and let I be an ideal of R. Then*

$$\frac{R[x]}{IR[x]} \cong \frac{R}{I}[x].$$

Solution. The map from $R \to R/I$ induces a map from $R[x]$ to $R/I[x]$ which sends the coefficients of each polynomial to their coset. Clearly this map is surjective. Its kernel is the set of polynomials whose coefficients are in I. That is, the kernel is $IR[x]$. The isomorphism follows. □

Problem .1.2. Let R be a ring, and let I be an ideal of R. Prove or disprove that if I is maximal in R, then $IR[x]$ is maximal in $R[x]$.

Solution. If I is maximal in R, then R/I is a field. By Lemma 4.1, the ring $R[x]/IR[x]$ is a polynomial ring over a field, or a PID. In particular, the polynomial $f(x) = x$ has no inverse so the ring is not a field and $IR[x]$ is not maximal in $R[x]$. It is, however, prime in $R[x]$ which is interesting in its own right. □

Problem .1.3. Let R be a PID, and let $f \in R[x]$. Prove that f is primitive if and only if it is very primitive. Prove that this is not necessarily the case in an arbitrary UFD.

Solution. If f is primitive, then for all principal prime ideals $\mathfrak{p}$, $f \notin \mathfrak{p}R[x]$. Since R is a PID, every prime ideal is principal. Thus, f is very primitive. The other direction follows from the definition.

For a counterexample in the more general case, consider the UFD $\mathbb{Z}[x]$ (note that we are only told this in §5.2 but we haven't proven it yet). Let $f = x + y \in \mathbb{Z}[x][y]$. Then f is primitive because $\gcd(x, y) = 1$ but $1 \notin (x, y)$ so $(x, y) \neq (1)$. In general, $d = \gcd(a_0, \ldots, a_d)$ does not imply that $(d) = (a_0, \ldots, a_d)$. □

Problem .1.4. Let R be a commutative ring, and let $f, g \in R[x]$. Prove that

$$fg \text{ is very primitive } \iff \text{ both } f \text{ and } g \text{ are very primitive.}$$

Solution. Suppose fg is very primitive. Then for all prime ideals $\mathfrak{p}$ in R, $fg \notin \mathfrak{p}R[x]$. That is, $f \notin \mathfrak{p}R[x]$ and $g \notin \mathfrak{p}R[x]$, or f is very primitive and g is very primitive. An equivalent reasoning proves the reverse direction. □

Problem .1.5. Prove Lemma 4.7.

Lemma 4.7. *Let R be a UFD, and let $f \in R[x]$. Then*

- $(f) = (\mathrm{cont}_f)(\underline{f})$*, where* $\underline{f}$ *is primitive;*
- *if* $(f) = (c)(g)$*, with* $c \in R$ *and* g *primitive, then* $(c) = (\mathrm{cont}_f)$*.*

Solution. Recall that cont_f is the gcd of the coefficients of f. Let $\underline{f}$ be the polynomial obtained by dividing each coefficient of f by cont_f. Then $(\mathrm{cont}_{\underline{f}}) = (1)$ since the remaining coefficients have no common factors. Thus, $\underline{f}$ is primitive and $(f) = (\mathrm{cont}_f)(\underline{f})$.

For the second point, note that we have $f = ucg$ for some unit $u \in R$. Then $\mathrm{cont}_f = \mathrm{cont}_{ucg} = uc$ since g is primitive. But then $(c) = (uc) = (\mathrm{cont}_f)$. □

Problem .1.6. Let R be a PID, and let K be its field of fractions.

- Prove that every element $c \in K$ can be written as a finite sum
$$c = \sum_i \frac{a_i}{p_i^{r_i}}$$
where the p_i are nonassociate irreducible elements in R, $r_i \geq 0$, and a_i, p_i are relatively prime.
- If $\sum_i \frac{a_i}{p_i^{r_i}} = \sum_j \frac{b_j}{q_j^{s_j}}$ are two such expressions, prove that (up to reshuffling) $p_i = q_i$, $r_i = s_i$, and $a_i \equiv b_i \mod p_i^{r_i}$.
- Relate this to the process of integration by 'partial fractions' you learned about when you took calculus.

Solution. Since R is a PID, it is in particular a UFD. Consider an element $c = \frac{x}{y}$. Then y has a unique factorization into non-associate irreducible elements (the p_i). Then we can write
$$\frac{x}{y} = \sum_i \frac{a_i}{p_i^{r_i}}$$
where the sum is guaranteed to have the same denominator by the way in which addition is defined in the field of fractions. To determine the a_i, note that expanding the sum on the right side yields a numerator whose terms are relatively prime. Thus, their gcd is a unit and since R is a PID, Bezout's identity holds. That is, there is a set of elements $a_1, \ldots, a_n$ which satisfy the equation $u = a_1 x_1 + \cdots + a_n x_n$ where x_i is y divided by the i-th irreducible factor and u is some unit. Multiplying both sides by $u^{-1}x$ yields a set of a_i which satisfy the equation above. Furthermore, they must be relatively prime to their corresponding p_i or the product with x_i would simply yield y.

With regards to the second point, I don't know that the expressions are always equivalent if the unique factorization of y is multiplied by a unit. However, the process described is precisely what occurs in partial fraction decomposition. Since R is a field, $R[x]$ is a PID. The elements of its field of fractions K can be written as above. □

Problem .1.7. A subset S of a commutative ring R is a *multiplicative subset* (or *multiplicatively closed*) if (i) $1 \in S$ and (ii) $s, t \in S \implies st \in S$. Define a relation on the set of pairs (a, s) with $a \in R, s \in S$ as follows:

$$(a, s) \sim (a', s') \iff (\exists t \in S), t(s'a - sa') = 0.$$

Note that if R is an integral domain and $S = R \setminus 0$, then S is a multiplicative subset, and the relation agrees with the relation introduced in §4.2.

- Prove that the relation $\sim$ is an *equivalence* relation.
- Denote by $\frac{a}{s}$ the equivalence class of (a, s), and define the same operations $+, \cdot$ on such 'fractions' as the ones introduced in the special case of §4.2. Prove that these operations are well-defined.
- The set $S^{-1}R$ of fractions, endowed with the operations $+, \cdot$, is the *localization of R at the multiplicative subset S* . Prove that $S^{-1}R$ is a commutative ring and that the function $a \mapsto \frac{a}{1}$ defines a ring homomorphism $\ell : R \to S^{-1}R$.
- Prove that $\ell(s)$ is invertible for every $s \in S$.
- Prove that $R \to S^{-1}R$ is initial among ring homomorphisms $f : R \to R'$ such that $f(s)$ is invertible in R' for every $s \in S$.
- Prove that $S^{-1}R$ is an integral domain if R is an integral domain.
- Prove that $S^{-1}R$ is the zero-ring if and only if $0 \in S$.

Solution. The relation is clearly reflexive. Let $t = 1$ and we find $t(sa - sa) = 0$ so $(a, s) \sim (a, s)$. Now suppose $(a, s) \sim (a', s')$. That is, there is a $t \in S$ such that $t(s'a - sa') = 0$. But then $-t(sa' - s'a) = 0$ so $t(sa' - s'a) = 0$. Thus, $(a', s') \sim (a, s)$. Finally, suppose $(a, s) \sim (a', s')$ and $(a', s') \sim (a'', s'')$. We have $t_1(s'a - sa') = 0$ and $t_2(s''a' - s'a'') = 0$. Then

$$s't_1t_2(s''a - sa'') = t_2s'' \cdot t_1(s'a - sa') + t_1s \cdot t_2(s''a' - s'a'') = 0$$

so the relation is transitive and hence an equivalence relation.

To verify that the operations are well-defined, suppose $(a_1, s_1) \sim (a_2, s_2)$. Then

$$t\left((s'a_1 + s_1a')(s_2s') - (s'a_2 - s_2a')(s_1s')\right) = (s')^2 \cdot t(a_1s_2 - a_2s_1) = 0$$

so addition is well-defined. Similarly,

$$t\left((s_2s')(a_1a') - (s_1s')(a_2a')\right) = a's' \cdot t(s_2a_1 - s_1a_2) = 0$$

so multiplication is well-defined.

To show that $S^{-1}R$ is a commutative ring, let $+, \cdot$ be the operations on the set of fractions. Clearly the set under $+$ forms a group with additive identity $\frac{0}{1}$ and inverses $-\frac{a}{s}$. Furthermore, we have

$$\frac{a}{s} + \frac{a'}{s'} = \frac{s'a + sa'}{ss'} = \frac{sa' + s'a}{s's} = \frac{a'}{s'} + \frac{a}{s}$$

so this group is abelian. Similarly, multiplication is commutative (assuming R is commutative). Lastly, we can see that distributivity holds since

$$\frac{a}{r}\left(\frac{b}{s}+\frac{c}{t}\right)=\frac{a}{r}\frac{(bt+cs)}{st}=\frac{abt}{rst}+\frac{acs}{rst}=\frac{a}{r}\cdot\frac{b}{s}+\frac{a}{r}\cdot\frac{c}{t}.$$

It is easy to verify that ℓ is a ring homomorphism since $\ell(a+b)=\frac{a+b}{1}=\frac{a}{1}+\frac{b}{1}=\ell(a)+\ell(b)$ and $\ell(a\cdot b)=\frac{ab}{1}=\frac{a}{1}\cdot\frac{b}{1}=\ell(a)\cdot\ell(b)$. The identity is also preserved. If $s\in S$, then $\ell(s)=\frac{s}{1}$. But we have $\frac{s}{1}\cdot\frac{1}{s}=1$ and $\frac{1}{s}\in S^{-1}R$ since $s\in S$. Thus, $\ell(s)$ is invertible.

To prove that $R\to S^{-1}R$ is initial among homomorphisms $f:R\to R'$ such that $f(s)$ is invertible in R' for $s\in S$, we need to define an induced homomorphism $\hat{f}:S^{-1}R\to R'$ such that the diagram

$$\begin{tikzcd}
S^{-1}R \arrow[rr, "\hat{f}"] & & R' \\
& R \arrow[ul, "\ell"] \arrow[ur, "f"'] &
\end{tikzcd}$$

commutes, and we must require that $\hat{f}$ is unique. Note that if $\hat{f}$ exists then we must have

$$\hat{f}\left(\frac{a}{s}\right)=\hat{f}\left(\frac{a}{1}\right)\hat{f}\left(\frac{1}{s}\right)=\hat{f}(\ell(a))\hat{f}(\ell(s)^{-1})=f(a)f(s)^{-1}$$

so the definition of $\hat{f}$ is unique. Furthermore, the definition $\hat{f}\left(\frac{a}{s}\right)=f(a)f(s)^{-1}$ is in fact a well-defined ring homomorphism from $S^{-1}R$ to R', showing that ℓ is initial.

Suppose that $S^{-1}R$ is not an integral domain. That is, there exist nonzero $\frac{a_1}{s_1},\frac{a_2}{s_2}$ whose product is zero. That is, we have

$$\frac{a_1a_2}{s_1s_2}=\frac{0}{1}\Longrightarrow(\exists t\in S),t(a_1a_2)=0$$

which can only occur if R is not an integral domain. The contrapositive is that if R is an integral domain then so is $S^{-1}R$.

First assume $0\in S$. Then $\ell(0)$ is invertible in $S^{-1}R$, say its inverse is r. But then we have $\ell(0)r=0\cdot r=1$ so $0=1$ implying that $S^{-1}R$ is the zero-ring. Now suppose $0\notin S$. Then 0 is not invertible in $S^{-1}R$ so $S^{-1}R$ is not the zero ring. $\square$

Problem .1.8. Let S be a multiplicative subset of a commutative ring R, as in Exercise 4.7. For every R-module M, define a relation $\sim$ on the set of pairs (m,s), where $m\in M$ and $s\in S$:

$$(m,s)\sim(m',s')\Longleftrightarrow(\exists t\in S),t(s'm-sm')=0.$$

Prove that this is an equivalence relation, and define an $S^{-1}R$-module structure on the set $S^{-1}M$ of equivalence classes, compatible with the R-module structure on M. The module $S^{-1}M$ is the *localization* of M at S.

Solution. This can be shown to be an equivalence relation in the same manner as above. To define an $S^{-1}R$-module structure on $S^{-1}M$, let

$$\frac{r}{s} \cdot \frac{m}{t} = \frac{r \cdot m}{st}.$$

Clearly this satisfies the definition of a module as

$$\frac{r}{s} \cdot \left(\frac{m_1}{t_1} + \frac{m_2}{t_2} \right) = \frac{r}{s} \cdot \frac{t_2 m_1 + t_1 m_2}{t_1 t_2} = \frac{r}{s} \cdot \frac{m_1}{s_1} + \frac{r}{s} \cdot \frac{m_2}{s_2}$$

The remaining axioms can be checked similarly. Furthermore, it is compatible with the R-module structure on M. $\square$

Problem .1.9. Let S be a multiplicative subset of a commutative ring R, and consider the localization operation introduced in Exercises 4.7 and 4.8.

- Prove that if I is an ideal of R such that $I \cap S = \emptyset$, then $I^e := S^{-1}I$ is a proper ideal of $S^{-1}R$.
- If $\ell : R \to S^{-1}R$ is the natural homomorphism, prove that if J is a proper ideal of $S^{-1}R$, then $J^c := \ell^{-1}(J)$ is an ideal of R such that $J^c \cap S = \emptyset$.
- Prove that $(J^c)^e = J$, while $(I^e)^c = \{a \in R \mid (\exists s \in S) sa \in I\}$.
- Find an example showing that $(I^e)^c$ need not equal I, even if $I \cap S = \emptyset$. (Hint: Let $S = \{1, x, x^2, \ldots\}$ in $R = \mathbb{C}[x, y]$. What is $(I^e)^c$ for $I = (xy)$?)

Solution. Clearly $0 \in S^{-1}I$ since $0 \in I$. Now let $\frac{a}{s}, \frac{b}{t} \in I^e$. Then

$$\frac{a}{s} - \frac{b}{t} = \frac{ta - sb}{st} \in I^e$$

since $ta - sb \in I$ and $st \in S$. Furthermore, let $\frac{r}{s} \in S^{-1}R$. Then

$$\frac{r}{s} \cdot \frac{a}{s'} = \frac{ra}{ss'} \in I^e$$

because $ra \in I$. Thus I^e is an ideal of $S^{-1}R$. Clearly it is proper because I does not contain any elements in S. Otherwise we would have $1 = \frac{s}{s} \in I^e$ and I^e would be all of $S^{-1}R$.

Now let J be a proper ideal of $S^{-1}R$. Since $0 \in J$, we have $\ell(0) = 0$ so $0 \in \ell^{-1}(J)$. Now suppose $a, b \in J^c$. Then $a - b = \ell^{-1}(\frac{a}{1}) - \ell^{-1}(\frac{b}{1}) \in J^c$. Similarly, it is closed under multiplication by R. Finally, suppose $J^c \cap S$ is nonempty. Then $\frac{s}{1} \in J$. But then $1 = \frac{1}{s} \cdot \frac{s}{1} \in J$ so J is all of $S^{-1}R$, a contradiction to it being proper. Thus, $J^c \cap S = \emptyset$.

Let $\frac{a}{s} \in (J^c)^e$. Then $\frac{a}{s} \in S^{-1}\ell^{-1}(J)$. In particular, $a \in \ell^{-1}(J)$ so $\frac{a}{1} \in J$. Therefore $\frac{a}{s} \in J$ so $(J^c)^e \subseteq J$. Now suppose $\frac{a}{s} \in J$. Then $a \in \ell^{-1}(J) = J^c$. It follows that $\frac{a}{s} \in (J^c)^e$ so $(J^c)^e = J$. Given an ideal $I \subseteq R$, suppose $a \in (I^e)^c$. Then $\ell(a) = \frac{a}{1} \in I^e = S^{-1}I$. In particular, $a \in I$ so $\subseteq$ holds. Now let $a \in R$ such that there is an $s \in S$ with $sa \in I$. Then $\ell(sa) \in I^e$ so $\frac{a}{1} \in I^e$. But then $a \in \ell^{-1}(I^e)$ showing that $\supseteq$ holds, meaning the two sets are equal.

Using the hint, consider the set $S = \{1, x, x^2, \ldots\}$ in the ring $R = \mathbb{C}[x, y]$. Clearly the ideal $I = (xy)$ does not intersect S since every nonzero element of I contains a factor of y. In fact, this means that $(I^e)^c = (y)$. □

Problem .1.10. With notation as in Exercise 4.9, prove that the assignment $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ gives an inclusion-preserving bijection between the set of *prime* ideals of R disjoint from S and the set of prime ideals of $S^{-1}R$. (Prove that $(\mathfrak{p}^e)^c = \mathfrak{p}$ if $\mathfrak{p}$ is a prime ideal disjoint from S.)

Solution. Let $\mathfrak{p}$ be a prime ideal disjoint from S. First we will show that $\mathfrak{p}^e$ is a prime ideal. Let $\frac{r}{s} \cdot \frac{a}{t} \in \mathfrak{p}^e$ with $\frac{r}{s} \notin \mathfrak{p}^e$. That is, $ra \in \mathfrak{p}$ but $r \notin \mathfrak{p}$ so $a \in \mathfrak{p}$. Since $t \in S$, we have $\frac{a}{t} \in \mathfrak{p}^e$, showing that it is prime. Now we must show the assignment is a bijection. Recall that $(\mathfrak{p}^e)^c = \{a \in R \mid (\exists s \in S) sa \in \mathfrak{p}\}$. However, since $s \notin \mathfrak{p}$, $sa \in \mathfrak{p}$ if and only if $a \in \mathfrak{p}$. In particular, $(\mathfrak{p}^e)^c = \mathfrak{p}$. Since $(\mathfrak{p}^c)^e = \mathfrak{p}$ as well, the assignment has a two-sided inverse and is a bijection. Finally, we show the bijection preserves inclusion. Suppose $\mathfrak{p} \subseteq \mathfrak{p}'$. Let $\frac{a}{s} \in \mathfrak{p}^e$. Since $a \in \mathfrak{p}'$ and $s \in S$, we have $\frac{a}{s} \in \mathfrak{p}'^e$. Thus, the inclusion is preserved. □

Problem .1.11. A ring is said to be *local* if it has a single maximal ideal.

Let R be a commutative ring, and let $\mathfrak{p}$ be a prime ideal of R. Prove that the set $S = R \setminus \mathfrak{p}$ is multiplicatively closed. The localization $S^{-1}R, S^{-1}M$ are then denoted $R_\mathfrak{p}, M_\mathfrak{p}$.

Prove that there is an inclusion-preserving bijection between the prime ideals of $R_\mathfrak{p}$ and the prime ideals of R contained in $\mathfrak{p}$. Deduce that $R_\mathfrak{p}$ is a local ring.

Solution. Since $\mathfrak{p}$ is a proper ideal, we have $1 \in R \setminus \mathfrak{p}$. Suppose $s, t \in S$. If $st \in \mathfrak{p}$ then one of $s, t \in \mathfrak{p}$, a contradiction. Thus, $st \in S$ so it is multiplicatively closed.

The assignment defined in Exercise 4.10 yields the desired inclusion-preserving bijection since a prime ideal contained in $\mathfrak{p}$ is obviously disjoint from S. Thus, the only maximal ideal is $\mathfrak{p}^e$. To show this, let I be an ideal in $R_\mathfrak{p}$. Then I is contained in some maximal ideal. If $\frac{a}{b} \in I$ with $a, b \in R \setminus \mathfrak{p}$ then $\frac{b}{a} \in R \setminus p$ so $\frac{a}{b} \cdot \frac{b}{a} = 1 \in I$ so $I = R_\mathfrak{p}$. Thus, $\mathfrak{p}R_\mathfrak{p}$ is the unique maximal ideal, meaning $R_\mathfrak{p}$ is a local ring. □

Problem .1.12. Let R be a commutative ring, and let M be an R-module. Prove that the following are equivalent:

- $M = 0$.
- $M_{\mathfrak{p}} = 0$ for every prime ideal $\mathfrak{p}$.
- $M_{\mathfrak{m}} = 0$ for every maximal ideal $\mathfrak{m}$.

(Hint: For the interesting implication, suppose that $m \neq 0$ in M; then the ideal $\{r \in R \mid rm = 0\}$ is proper. By Proposition 3.5, it is contained in a maximal ideal $\mathfrak{m}$. What can you say about $M_{\mathfrak{m}}$.

Solution. Suppose $M = 0$. For a prime ideal $\mathfrak{p}$, we have $M_{\mathfrak{p}} = \{\frac{a}{b} \mid a \in M, b \in R \setminus \mathfrak{p}\} = \{0\}$ since the only element of M is 0. The second statement clearly implies the third since every maximal ideal $\mathfrak{m}$ is prime. To show the third point implies the first, suppose $m \neq 0$ in M. The ideal specified in the hint is proper so it is contained in a maximal ideal $\mathfrak{m}$. Then $M_{\mathfrak{m}} = \{\frac{a}{b} \mid a \in M, b \in R \setminus \mathfrak{m}\}$ contains the nonzero element $\frac{m}{1}$. Thus, if $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$, then $M = 0$, showing that all of the listed properties are equivalent. $\square$

Problem .1.13. Let k be a field, and let v be a discrete valuation on k. Let R be the corresponding DVR, with local parameter t (see Exercise 2.20).

- Prove that R is local, with maximal ideal $\mathfrak{m} = (t)$. (Hint: Note that every element of $R \setminus \mathfrak{m}$ is invertible.)
- Prove that k is the field of fractions of R.
- Now let A be a PID, and let $\mathfrak{p}$ be a prime ideal in A. Prove that the localization $A_{\mathfrak{p}}$ is a DVR. (Hint: If $\mathfrak{p} = (p)$, define a valuation on the field of fractions of A in terms of 'divisibility by p'.)

Solution. First, recall that a local parameter $t \in R$ is an element such that $v(t) = 1$. We have shown in Exercise 2.20 that local parameters have the property that for any nonzero ideal I of R, we have $I = (t^k)$ for some $k \geq 1$. Thus, $I \subseteq (t)$ so (t) is the unique maximal ideal and R is local. Alternatively, suppose $a \in I$ is not divisible by t. If $v(a) > 0$ then $v(a/t) = v(a) - v(t) \geq 0$ so $a/t \in R$. Thus, $v(a) = 0$. Furthermore, $v(a^{-1}) = -v(a) = 0$ so $a^{-1} \in R$ and a is invertible. Therefore, $1 = a \cdot a^{-1} \in I$ so $I = R$.

Let K denote the field of fractions of R. There is an obvious embedding $f : R \to k$ so by the universal property of the field of fractions, there is an injective homomorphism $\hat{f} : K \to k$. To show the fields are isomorphic, we construct an explicit isomorphism. Consider $g : k \to K$ letting $g(a) = \frac{a}{1}$. Clearly g is a homomorphism so it is injective. To show that it is surjective, let $\frac{a}{b} \in K$. Then $\frac{a}{b} = \frac{ab^{-1}}{bb^{-1}} = g(ab^{-1})$ so the image of g is all of K. Thus, k is the field of fractions of R.

Let $\mathfrak{p} = (p)$. The localization $A_{\mathfrak{p}} = \{\frac{a}{b} \mid a \in A, b \in A \setminus \mathfrak{p}\}$. Since A is a PID, it is also a UFD so elements of $A_{\mathfrak{p}}$ can be expressed as $\frac{p^k a'}{b}$ for some $k \geq 0$. This is a generalization of the p-adic valuation defined over the rationals in Exercise 2.19. $\square$

Problem .1.14. With notation as in Exercise 4.8, define operations $N \mapsto N^e$ and $\hat{N} \mapsto \hat{N}^c$ for submodules $N \subseteq M$, $\hat{N} \subseteq S^{-1}M$, respectively, analogously to the operations defined in Exercise 4.9. Prove that $(\hat{N})^c)^e = \hat{N}$. Prove that every localization of a Noetherian module is Noetherian.

In particular, all localizations $S^{-1}R$ of a Noetherian ring are Noetherian.

Solution. Let $\frac{a}{s} \in \hat{N}$. Then $a \in \ell^{-1}(\hat{N})$ so $\frac{a}{s} \in (\hat{N}^c)^e$. Now suppose $\frac{a}{s} \in (\hat{N}^c)^e$. Then $a \in \hat{N}^c$ so $a \in \ell^{-1}(\hat{N})$. That is, $\frac{a}{1} \in \hat{N}$. But then $\frac{1}{s} \cdot \frac{a}{1} = \frac{a}{s} \in \hat{N}$. Thus, $(\hat{N}^c)^e = \hat{N}$.

Consider a chain of ascending submodules

$$S^{-1}M_1 \subset S^{-1}M_2 \subset \cdots$$

of $S^{-1}N$ for some Noetherian module N. Then we can take the mapping $\hat{N} \mapsto \hat{N}^c$ for each submodule in the chain to obtain the chain

$$M_1 \subset M_2 \subset \cdots$$

which stabilizes since N is Noetherian. Thus, the original chain also stabilizes and $S^{-1}N$ is Noetherian. □

Problem .1.15. Let R be a UFD, and let S be a multiplicatively closed subset of R (cf. Exercise 4.7).

- Prove that if q is irreducible in R, then $q/1$ is either irreducible or a unit in $S^{-1}R$.
- Prove that if a/s is irreducible in $S^{-1}R$, then a/s is an associate of $q/1$ for some irreducible element q of R.
- Prove that $S^{-1}R$ is also a UFD.

Solution. Let q be an irreducible element of R. If q divides some element of S, say $s = qr$, then $q/1$ is a unit because

$$\frac{q}{1} \cdot \frac{r}{s} = \frac{qr}{s} = 1.$$

Now suppose q does not divide any element of S. If $q/1$ factorizes in $S^{-1}R$, then we have $\frac{q}{1} = \frac{a}{s} \cdot \frac{b}{s'}$. That is, there is some $t \in S$ such that

$$tqss' = tab.$$

Since R is a UFD, and there is only one factor of q on the left hand side, there is also only one factor of q on the right hand side. WLOG, say q divides a. Then the irreducible elements in the factorization of b divide elements of S. Thus $\frac{b}{s'}$ is a unit (by case one) and $\frac{1}{q}$ is irreducible.

Consider a factorization $\frac{a}{s} = \frac{q}{1} \cdot \frac{b}{t}$ for some irreducible element q. Since $\frac{a}{s}$ is irreducible, one of the factors is a unit. If $\frac{b}{t}$ is a unit, then $(\frac{q}{1}) = (\frac{a}{s})$. If $\frac{q}{1}$ is a unit, then so is $\frac{q}{t}$. In particular, we can rewrite the factorization as $\frac{a}{s} = \frac{q}{t} \cdot \frac{b}{1}$. Finally, b is irreducible in R because if it were not then $\frac{b}{1}$ would not be irreducible in $S^{-1}R$. Thus, $(\frac{a}{s}) = (\frac{b}{1})$ for an irreducible b.

Let $\frac{a}{s} \in S^{-1}R$. Suppose $a = u(p_1^{b_1} \cdots p_r^{b_r})(q_1^{c_1} \cdots q_t^{c_t})$ where the p_i are irreducible elements which divide elements in S and the q_i are irreducible elements which do not divide elements in S. Then we have

$$\frac{a}{s} = \frac{u}{s} \cdot \frac{p_1^{b_1}}{1} \cdots \frac{p_r^{b_r}}{1} \cdot \frac{q_1^{c_1}}{1} \cdots \frac{q_t^{c_t}}{1}$$

is a factorization of $\frac{a}{s}$ into a unit multiplied by a product of irreducibles (by the first point). Uniqueness follows from multiplying factors by a unit and using the second point. □

Problem .1.16. Let R be a Noetherian integral domain, and let $s \in R$, $s \neq 0$, be a prime element. Consider the multiplicatively closed subset $S = \{1, s, s^2, \ldots\}$. Prove that R is a UFD if and only if $S^{-1}R$ is a UFD. (Hint: By Exercise 2.10, it suffices to show that every prime of height 1 is principal. Use Exercise 4.10 to relate prime ideals in R to prime ideals in the localization.)

On the basis of results such as this and of Exercise 4.15, one might suspect that being factorial is a local property, that is, that R is a UFD if and only if $R_{\mathfrak{p}}$ is a UFD for all primes $\mathfrak{p}$, if and only if $R_{\mathfrak{m}}$ is a UFD for all maximals $\mathfrak{m}$. This is regrettably not the case. A ring R is *locally factorial* if $R_{\mathfrak{m}}$ is a UFD for all maximal ideals $\mathfrak{m}$; factorial implies locally factorial by Exercise 4.15, but locally factorial rings that are not factorial do exist.

Solution. We have shown that if R is a UFD then $S^{-1}R$ is also a UFD. To show the converse, let $\mathfrak{p}$ be a prime ideal of height 1 in R. There is a corresponding prime ideal $\mathfrak{p}^e \in S^{-1}R$ which also has height 1. If $S^{-1}R$ is a UFD then $\mathfrak{p}^e$ is principal. But then $\mathfrak{p}$ is principal as well, so R is a UFD. □

Problem .1.17. Let F be a field, and recall the notion of *characteristic* of a ring; the characteristic of a field is either 0 or a prime integer (Exercise III.3.14.)

- Show that F has characteristic 0 if and only if it contains a copy of $\mathbb{Q}$ and that F has characteristic p if and only if it contains a copy of the field $\mathbb{Z}/p\mathbb{Z}$.
- Show that (in both cases) this determines the smallest subfield of F; it is called the *prime subfield* of F.

Solution. Recall that the characteristic of a ring is the smallest nonnegative integer such that $n \cdot 1 = 0$. Suppose a field F contains a copy of $\mathbb{Q}$ and consider the homomorphism $f : \mathbb{Z} \to F$, $f(a) = a \cdot 1$. Let n denote the characterstic of the ring. If $n > 0$ then $f(n) = n \cdot 1 = 0$. However, $n \neq 0$ in F since $n \neq 0$ in $\mathbb{Q}$. Therefore, $n = 0$. Now suppose F has characteristic 0. Then there is an injective homomorphism $f : \mathbb{Z} \to F$. That is, there is an embedding of $\mathbb{Z}$ into K so K contains the inverses of the integers as well. Thus, K contains the field of fractions of $\mathbb{Z}$ which is isomorphic to $\mathbb{Q}$.

Now suppose a field F contains $\mathbb{Z}/p\mathbb{Z}$ and consider the homomorphism $f : \mathbb{Z} \to F, f(a) = a \cdot 1$. Let n denote the characteristic of F. Then $n \leq p$ since $f(p) = p \cdot 1 = 0$. If $n < p$ and $n \cdot 1 = 0$, we arrive at a contradiction since this does not hold in $\mathbb{Z}/p\mathbb{Z}$. Thus, $n = p$. Now suppose F has characteristic p and consider the homomorphism $f : \mathbb{Z} \to F$. The homomorphism has kernel $p\mathbb{Z}$. By the first isomorphism theorem,

$$\frac{\mathbb{Z}}{p\mathbb{Z}} \cong \text{im} f \subseteq F$$

completing the proof. Note that in both cases, the desired subfield is generated by 1.

Consider the intersection of all subfields of F, denoted by K. Certainly $1 \in K$. If $\text{char}(F) = p$ then K contains the subfield generated by 1 which we have shown is isomorphic $\mathbb{Z}/p\mathbb{Z}$. Similarly, if $\text{char}(F) = 0$ then K contains $\mathbb{Z}$ and its multiplicative inverses which is isomorphic to $\mathbb{Q}$. The reverse inclusion is obvious, completing the proof. □

Problem .1.18. Let R be an integral domain. Prove that the invertible elements in $R[x]$ are the units of R, viewed as constant polynomials.

Solution. Certainly the units of R are invertible in $R[x]$. To show that these are the only invertible elements, suppose $fg = 1$. Since R is a domain, we have the identity $\deg(fg) = \deg(f) + \deg(g)$. It follows that f and g are constant and thus are units in R. □

Problem .1.19. An element $a \in R$ in a ring is said to be *nilpotent* if $a^n = 0$ for some $n \geq 0$. Prove that if a is nilpotent, then $1 + a$ is a unit in R.

Solution. Suppose a is nilpotent, say $a^n = 0$. Then

$$(1 + a)(1 - a + a^2 - \cdots + (-1)^{n-1}a^{n-1}) = 1$$

so $1 + a$ is invertible. □

Problem .1.20. Generalize the result of Exercise 4.18 as follows: let R be a commutative ring, and let $f = a_0 + a_1x + \cdots + a_dx^d \in R[x]$; prove that f is a unit in $R[x]$ if and only if a_0 is a unit in R and $a_1, \ldots, a_d$ are nilpotent. (Hint: If $b_0 + b_1x + \cdots + b_ex^e$ is the inverse of f, show by induction that $a_d^{i+1}b_{e-i} = 0$ for all $i \geq 0$, and deduce that a_d is nilpotent.)

Solution. First, note that if an element a is nilpotent, then so is ra for all $r \in R$. Furthermore, given a unit a_0 and a nilpotent element a_1, we have $a_0 + a_1 = a_0(1 + a_0^{-1}a_1)$ which is the product of two units and thus a unit itself.

We do a proof by induction for both directions. Suppose a_0 is a unit and a_i is nilpotent for $i > 0$. In the case $n = 1$, we have shown above that $a_0 + a_1x$ is a unit. Now suppose this holds for $n = k$ and let $n = k + 1$. Consider the polynomial $p(x) = a_0 + a_1x + \cdots a_{k+1}x^{k+1}$. By the hypothesis, $f(x) = a_0 + a_1x + \cdots a_kx^k$ is a unit. Furthermore, $a_{k+1}x^{k+1}$ is nilpotent. Since the sum of a unit and a nilpotent element is a unit, $p(x)$ must be a unit.

For the reverse direction, suppose f is a unit with inverse g. Clearly $a_0b_0 = 1$. Thus, a_0 and b_0 are both units. To show that $a_d^{i+1}b_{e-i} = 0$ for $i \geq 0$, we induct on i. For the case $i = 0$, the statement clearly holds as a_db_e is the leading term of fg. For $i > 0$, the coefficient of x^{d+e-i} is

$$a_db_{e-i} + a_{d-1}b_{e-i+1} + \cdots + a_{d-i}b_e.$$

Multiplying through by a_d^i and applying the induction hypothesis proves the result. In particular, letting $i = e$ and using the fact that b_0 is a unit shows that a_d is nilpotent. Therefore $f - a_dx^d$ is a unit (by the first part of this solution). Repeating allows us to conclude that all a_i for $i > 0$ are nilpotent. □

Problem .1.21. Establish the characterization of irreducible polynomials over a UFD given in Corollary 4.17.

Corollary 4.17. *Let R be a UFD and K the field of fractions of R. Let $f \in R[x]$ be a nonconstant polynomial. Then f is irreducible in $R[x]$ if and only if it is irreducible in $K[x]$ and primitive.*

Solution. One direction is proven in the chapter so we prove the other to establish the characterization. Suppose $f \in R[x]$ is irreducible in $K[x]$ and primitive. Assume $f = gh$ for $g, h \in R[x]$. The irreducibility of f in $K[x]$ implies that one of g, h is a unit in $K[x]$, say g. By Exercise 4.18, g has degree 0 so $\text{cont}(g) = g$. But then $1 = \text{cont}(f) = \text{cont}(g)\text{cont}(h)$ so g is a unit in R, implying that f is irreducible in $R[x]$. □

Problem .1.22. Let k be a field, and let f, g be two polynomials in $k[x, y] = k[x][y]$. Prove that if f and g have a nontrivial common factor in $k(x)[y]$, then they have a nontrivial common factor in $k[x, y]$.

Solution. Recall that $k(x)$ is the field of fractions of $k[x]$. Suppose f and g have a nontrivial common factor in $k(x)[y]$, say h. We can choose $c \in k(x)$ such that $h = ch'$ where $h' \in k[x, y]$. But then h' is a nontrivial factor of f and g. □

Problem .1.23. Let R be a UFD, K its field of fractions, $f(x) \in R[x]$, and assume $f(x) = \alpha(x)\beta(x)$ with $\alpha(x), \beta(x)$ in $K[x]$. Prove that there exists a $c \in K$ such that $c\alpha(x) \in R[x]$, $c^{-1}\beta(x) \in R[x]$, so that

$$f(x) = (c\alpha(x))(c^{-1}\beta(x))$$

splits $f(x)$ as a product of factors in $R[x]$.

Deduce that if $\alpha(x)\beta(x) = f(x) \in R[x]$ is monic and $\alpha(x) \in K[x]$ is monic, then $\alpha(x), \beta(x)$ are both in $R[x]$ and $\beta(x)$ is also monic.

Solution. First note that if f is not primitive then we can factor out the content and let $c = 1$ so we may assume f is primitive. Let $a, b \in K$ such that

$$\alpha = a\underline{\alpha}, \quad \beta = b\underline{\beta}$$

where $\underline{\alpha}, \underline{\beta}$ are primitive in $R[x]$. Note that by Gauss' lemma, ab is a unit in R. Then there exists a unit $u \in R$ such that $a = b^{-1}u$. Now let $c = a^{-1}$ and $c^{-1} = b^{-1}u$. Then we find $c\alpha = a^{-1}\alpha = \underline{\alpha} \in R[x]$. Similarly, $c^{-1}\beta = b^{-1}u\beta = u\underline{\beta} \in R[x]$. Then we find

$$(c\alpha)(c^{-1}\beta) = u\underline{\alpha}\underline{\beta} = ab\underline{\alpha}\underline{\beta} = f$$

so we are done.

We deduce that if f and α are monic, then β is monic as well so that the leading coefficient of f is 1. Furthermore, suppose $\alpha \notin R[x]$. Then there exists an element $c \in K$ such that $c\alpha \in R[x]$. Note that c is not a unit in R or else $\alpha \in R[x]$. But then the leading coefficient of $c^{-1}\beta$ is c^{-1} so $c^{-1}\beta \notin R[x]$. Similar reasoning shows that both $\alpha, \beta \in R[x]$. $\square$

Problem .1.24. In the same situation as in Exercise 4.23, prove that the product of any coefficient of α with any coefficient of β lies in R.

Solution. Let α_i, β_i denote the i-th coefficient of α, β respectively. Using the result of the previous exercise, we have $c\alpha_i, c^{-1}\beta_i \in R$ for all i. Then $\alpha_i\beta_j = c\alpha_i \cdot c^{-1}\beta_j \in R$ for all i, j. $\square$

Problem .1.25. Prove *Fermat's last theorem for polynomials:* the equation

$$f^n + g^n = h^n$$

has no solutions in $\mathbb{C}[t]$ for $n > 2$ and f, g, h not all constant. (Hint: First, prove that f, g, h may be assumed to be relatively prime. Next, the polynomial $1 - t^n$ factorizes in $\mathbb{C}[t]$ as $\prod_{i=1}^{n}(1-\zeta^i t)$ for $\zeta = e^{2\pi i/n}$; deduce that $f^n = \prod_{i=1}^{n}(h-\zeta^i g)$. Use unique factorization in $\mathbb{C}[t]$ to conclude that each of the factors $h - \zeta^i g$ is an n-th power. Now let $h - g = a^n$, $h - \zeta g = b^n$, $h - \zeta^2 g = c^n$ (this is where the

$n > 2$ hypothesis enters). Use this to obtain a relation $(\lambda a)^n + (\mu b)^n = (\nu c)^n$, where λ, μ, ν are suitable complex numbers. What's wrong with this?)

The same pattern of proof would work in any environment where unique factorization is available; if adjoining to $\mathbb{Z}$ a primitive n-th root of 1 and roots of other elements as needed in this argument led to a unique factorization domain, the full-fledged Fermat's last theorem would be as easy to prove as indicated in this exercise. This is not the case, a fact famously missed by G. Lamé as he announced a 'proof' of Fermat's last theorem to the Paris Academy on March 1, 1847.

Solution. First, note that if f, g, h have a common factor c then $(f/c)^n + (g/c)^n = (h/c)^n$ is another solution. Thus, we may assume that f, g, h are relatively prime. If we consider K to be the field of fractions of $\mathbb{C}[t]$ then we have

$$1 - \left(\frac{g}{h}\right)^n = \prod_{i=1}^{n} \left(1 - \zeta^i \frac{g}{h}\right).$$

Multiplying both sides by h^n yields the factorization $f^n = h^n - g^n = \prod_{i=1}^{n}(h - \zeta^i g)$. Now we show that $(h - \zeta^i g)$ is coprime to $(h - \zeta^j g)$ for $i \neq j$. Indeed, we find that

$$h - \zeta^i g - (h - \zeta^j g) = (\zeta^j - \zeta^i) g$$
$$h - \zeta^i g + \frac{\zeta^i}{\zeta^j - \zeta^i} \left(\zeta^j - \zeta^i\right) g = h$$

Since $\mathbb{C}[t]$ is a Euclidean domain, we have $\gcd(h - \zeta^i g, h - \zeta^j g) = \gcd(g, h) = 1$. Thus, the factors are all coprime.

In any UFD, if the product of coprime factors is an n-th power, then each factor is an n-th power. We prove this by induction on the number of prime factors of c which we denote by k. Indeed, suppose a, b are coprime and let $ab = c^n$. If $k = 0$ then c is a unit so a, b are units multiplied by 1^n. If $k > 0$ then there is a prime $p \mid c$ so $p^n \mid c^n = ab$. Therefore, $p^n \mid a$ or $p^n \mid b$ since a, b are coprime. WLOG, assume the latter. We find $a(b/p^n) = (c/p)^n$. Since c/p has fewer prime factors than c, the inductive hypothesis applies and $a = r^n, b/p^n = s^n \implies b = (ps)^n$. Thus, we have shown that we can write $h - g = a^n, h - \zeta g = b^n, h - \zeta^2 g = c^n$ for $a, b, c \in \mathbb{C}[t]$.

With this, we can derive the following.

$$g = \frac{1}{1-\zeta}(b^n - a^n)$$
$$h = \frac{1}{1-\zeta}(b^n - \zeta a^n)$$

$$\zeta a^n + (1+\zeta) b^n = c^n$$

Since $\mathbb{C}$ is an algebraically closed field, there exist $x, y \in \mathbb{C}$ such that $x^n = \zeta$ and $y^n = 1 + \zeta$. Thus, we can write $(ax)^n + (by)^n = c^n$. But then we find $\max(\deg a, \deg b, \deg c) \leq \max(\deg f, \deg g, \deg h)/n < \max(\deg f, \deg g, \deg h)$. If we take a solution f, g, h to the initial equation such that the maximum degree is minimal among all solutions, then we arrive at a contradiction since we have constructed another solution of lower degree. $\square$