12. Polynomials over UFDs

The goal here is to give a general result which has as corollary that that rings of polynomials in several variables

$$k[x_1, \ldots, x_n]$$

with coefficients in a field k are *unique factorization domains* in a sense made precise just below. Similarly, polynomial rings in several variables

$$\mathbb{Z}[x_1, \ldots, x_n]$$

with coefficients in $\mathbb{Z}$ form a unique factorization domain. [1]

---

1. *Gauss' lemma*

A **factorization** of an element r into *irreducibles* in an integral domain R is an expression for r of the form

$$r = u \cdot p_1^{e_1} \ldots p_m^{e_m}$$

where u is a unit, p_1 through p_m are *non-associate* [2] irreducible elements, and the e_is are positive integers. Two factorizations

$$r = u \cdot p_1^{e_1} \ldots p_m^{e_m}$$

$$r = v \cdot q_1^{f_1} \ldots q_n^{f_n}$$

[1] Among other uses, these facts are used to discuss Vandermonde determinants, and in the proof that the *parity* (or *sign*) of a permutation is well-defined.

[2] Recall that two elements x, y of a commutative ring R are *associate* if $x = yu$ for some unit u in R. This terminology is most often applied to prime or irreducible elements.

into irreducibles p_i and q_j with units u, v are **equivalent** if $m = n$ and (after possibly renumbering the irreducibles) q_i is *associate* to p_i for all indices i. A domain R is a **unique factorization domain** (UFD) if any two factorizations are equivalent.

[1.0.1] Theorem: (*Gauss*) Let R be a unique factorization domain. Then the polynomial ring in one variable $R[x]$ is a unique factorization domain.

[1.0.2] Remark: The proof factors $f(x) \in R[x]$ in the larger ring $k[x]$ where k is the *field of fractions* of R (see below), and rearranges constants to get coefficients into R rather than k. Uniqueness of the factorization follows from uniqueness of factorization in R and uniqueness of factorization in $k[x]$.

[1.0.3] Corollary: A polynomial ring $k[x_1, \ldots, x_n]$ in a finite number of variables $x_1, \ldots, x_n$ over a field k is a unique factorization domain. (*Proof by induction.*) ///

[1.0.4] Corollary: A polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$ in a finite number of variables $x_1, \ldots, x_n$ over the integers $\mathbb{Z}$ is a unique factorization domain. (*Proof by induction.*) ///

Before proving the theorem itself, we must verify that unique factorization recovers some naive ideas about divisibility. Recall that for $r, s \in R$ not both 0, an element $g \in R$ dividing both r and s such that any divisor d of both r and s also divides g, is a **greatest common divisor** of r and s, denoted $g = \gcd(r, s)$.

[1.0.5] Proposition: Let R be a unique factorization domain. For r, s in R not both 0 there exists $\gcd(r, s)$ unique up to an element of $R^\times$. Factor both r and s into irreducibles

$$r = u \cdot p_1^{e_1} \ldots p_m^{e_m} \qquad s = v \cdot p_1^{f_1} \ldots p_m^{f_n}$$

where u and v are units and the p_i are mutually non-associate irreducibles (allow the exponents to be 0, to use a common set of irreducibles to express both r and s). Then the greatest common divisor has exponents which are the minima of those of r and s

$$\gcd(r, s) = p_1^{\min(e_1, f_1)} \ldots p_m^{\min(e_m, f_m)}$$

Proof: Let

$$g = p_1^{\min(e_1, f_1)} \ldots p_m^{\min(e_m, f_m)}$$

First, g does divide both r and s. On the other hand, let d be any divisor of both r and s. Enlarge the collection of inequivalent irreducibles p_i if necessary such that d can be expressed as

$$d = w \cdot p_1^{h_1} \ldots p_m^{h_m}$$

with unit w and non-negative integer exponents. From $d|r$ there is $D \in R$ such that $dD = r$. Let

$$D = W \cdot p_1^{H_1} \ldots p_m^{H_m}$$

Then

$$wW \cdot p_1^{h_1+H_1} \ldots p_m^{h_m+H_m} = d \cdot D = r = u \cdot p_1^{e_1} \ldots p_m^{e_m}$$

Unique factorization and non-associateness of the p_i implies that the exponents are the same: for all i

$$h_i + H_i = e_i$$

Thus, $h_i \leq e_i$. The same argument applies with r replaced by s, so $h_i \leq f_i$, and $h_i \leq \min(e_i, f_i)$. Thus, $d|g$. For uniqueness, note that any other greatest common divisor h would have $g|h$, but also $h|r$ and $h|s$. Using the unique (up to units) factorizations, the exponents of the irreducibles in g and h must be the same, so g and h must differ only by a unit. ///

[1.0.6] **Corollary:** Let R be a unique factorization domain. For r and s in R, let $g = \gcd(r, s)$ be the greatest common divisor. Then $\gcd(r/g,\, s/g) = 1$. ///

---

2. *Fields of fractions*

The **field of fractions** k of an integral domain R is the collection of fractions a/b with $a, b \in R$ and $b \neq 0$ and with the usual rules for addition and multiplication. More precisely, k is the set of ordered pairs (a, b) with $a, b \in R$ and $b \neq 0$, modulo the equivalence relation that

$$(a, b) \sim (c, d)$$

if and only if $ad - bc = 0$. [3] Multiplication and addition are [4]

$$(a, b) \cdot (c, d) = (ac, bd)$$

$$(a, b) + (c, d) = (ad + bc, bd)$$

The map $R \longrightarrow k$ by $r \longrightarrow (r, 1)/\sim$ is readily verified to be a ring homomorphism. [5] Write a/b rather than $(a, b)/\sim$. When R is a unique factorization ring, whenever convenient suppose that fractions a/b are *in lowest terms*, meaning that $\gcd(a, b) = 1$.

Extend the notions of divisibility to apply to elements of the fraction field k of R. [6] First, say that $x|y$ for two elements x and y in k if there is $r \in R$ such that $s = rx$. [7] And, for $r_1, \ldots, r_n$ in k, not all 0, a greatest common divisor $\gcd(r_1, \ldots, r_n)$ is an element $g \in k$ such that g divides each r_i and such that if $d \in k$ divides each r_i then $d|g$.

[2.0.1] **Proposition:** In the field of fractions k of a unique factorization domain R (extended) greatest common divisors exist.

Proof: We reduce this to the case that everything is inside R. Given elements $x_i = a_i/b_i$ in k with a_i and b_i all in R, take $0 \neq r \in R$ such that $rx_i \in R$ for all i. Let G be the greatest common divisor of the rx_i, and put $g = G/r$. We claim this g is the greatest common divisor of the x_i. On one hand, from $G|rx_i$ it follows that $g|x_i$. On the other hand, if $d|x_i$ then $rd|rx_i$, so rd divides $G = rg$ and $d|g$. ///

The **content** $\mathrm{cont}(f)$ of a polynomial f in $k[x]$ is the greatest common divisor [8] of the coefficients of f.

[2.0.2] **Lemma:** *(Gauss)* Let f and g be two polynomials in $k[x]$. Then

$$\mathrm{cont}(fg) = \mathrm{cont}(f) \cdot \mathrm{cont}(g)$$

---

[3] This corresponds to the ordinary rule for equality of two fractions.

[4] As usual for fractions.

[5] The assumption that R is a *domain*, is needed to make this work so simply. For commutative rings (with 1) with proper 0-divisors the natural homomorphism $r \longrightarrow (r, 1)$ of the ring to its field of fractions will not be injective. And this construction will later be seen to be a simple extreme example of the more general notion of *localization* of rings.

[6] Of course notions of divisibility in a field itself are trivial, since any non-zero element divides any other. This is *not* what is happening now.

[7] For non-zero r in the domain R, $rx|ry$ if and only if $x|y$. Indeed, if $ry = m \cdot rx$ then by cancellation (using the domain property), $y = m \cdot x$. And $y = m \cdot x$ implies $ry = m \cdot rx$ directly.

[8] The values of the content function are only well-defined up to units $R^\times$. Thus, Gauss' lemma more properly concerns the *equivalence classes* of irreducibles dividing the respective coefficients.

Proof: From the remark just above for any $c \in k^\times$

$$\mathrm{cont}(c \cdot f) = c \cdot \mathrm{cont}(f)$$

Thus, since

$$\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}) = 1$$

without loss of generality $\mathrm{cont}(f) = 1$ and $\mathrm{cont}(g) = 1$. Thus, in particular, both f and g have coefficients in the ring R. Suppose $\mathrm{cont}(fg) \neq 1$. Then there is non-unit irreducible $p \in R$ dividing all the coefficients of fg. Put

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots$$

$$g(x) = b_0 + b_1 x + b_2 x^2 + \ldots$$

But p does not divide *all* the coefficients of f, nor *all* those of g. Let i be the smallest integer such that p does not divide a_i, j the largest integer such that p does not divide b_j, and consider the coefficient of x^{i+j} in fg. It is

$$a_0 b_{i+j} + a_1 b_{i+j-1} + \ldots + a_{i-1} b_{j-1} + a_i b_j + a_{i+1} b_{j-1} + \ldots + a_{i+j-1} b_1 + a_{i+j} b_0$$

In summands to the left of $a_i b_j$ the factor a_k with $k < i$ is divisible by p, and in summands to the right of $a_i b_j$ the factor b_k with $k < j$ is divisible by p. This leaves only the summand $a_i b_j$ to consider. Since the whole sum is divisible by p, it follows that $p|a_i b_j$. Since R is a unique factorization domain, either $p|a_i$ or $p|b_j$, contradiction. Thus, it could not have been that p divided all the coefficients of fg. ///

[2.0.3] **Corollary:** Let f be a polynomial in $R[x]$. If f factors properly in $k[x]$ then f factors properly in $R[x]$. More precisely, if f factors as $f = g \cdot h$ with g and h polynomials in $k[x]$ of positive degree, then there is $c \in k^\times$ such that $cg \in R[x]$ and $h/c \in R[x]$, and

$$f = (cg) \cdot (h/c)$$

is a factorization of f in $R[x]$.

Proof: Since f has coefficients in R, $\mathrm{cont}(f)$ is in R. By replacing f by f/c we may suppose that $\mathrm{cont}(f) = 1$. By Gauss' lemma

$$\mathrm{cont}(g) \cdot \mathrm{cont}(h) = \mathrm{cont}(f) = 1$$

Let $c = \mathrm{cont}(g)$. Then $\mathrm{cont}(h) = 1/c$, and $\mathrm{cont}(g/c) = 1$ and $\mathrm{cont}(c \cdot h) = 1$, so g/c and ch are in $R[x]$, and $(g/c) \cdot (ch) = f$. Thus f is reducible in $R[x]$. ///

[2.0.4] **Corollary:** The irreducibles in $R[x]$ are of two sorts, namely irreducibles in R and polynomials f in $R[x]$ with $\mathrm{cont}(f) = 1$ which are irreducible in $k[x]$.

Proof: If an irreducible p in R factored in $R[x]$ as $p = gh$, then the degrees of g and h would be 0, and g and h would be in R. The irreducibility of p in R would imply that one of g or h would be a unit. Thus, irreducibles in R remain irreducible in $R[x]$.

Suppose p was irreducible in $R[x]$ of positive degree. If $g = \mathrm{cont}(p)$ was a non-unit, then $p = (p/g) \cdot g$ would be a proper factorization of p, contradiction. Thus, $\mathrm{cont}(p) = 1$. The previous corollary shows that p is irreducible in $k[x]$.

Last suppose that f is irreducible in $k[x]$, and has $\mathrm{cont}(f) = 1$. The irreducibility in $k[x]$ implies that if $f = gh$ in $R[x]$ then the degree one of g or h must be 0. Without loss of generality suppose $\deg g = 0$, so $\mathrm{cont}(g) = g$. Since

$$1 = \mathrm{cont}(f) = \mathrm{cont}(g)\mathrm{cont}(h)$$

g is a unit in R, so $f = gh$ is not a proper factorization, and f is irreducible in $R[x]$. ///

Proof: (*of theorem*) We can now combine the corollaries of Gauss' lemma to prove the theorem. Given a polynomial f in $R[x]$, let $c = \mathrm{cont}(f)$, so from above $\mathrm{cont}(f/c) = 1$. The hypothesis that R is a unique factorization domain allows us to factor u into irreducibles in R, and we showed just above that these irreducibles remain irreducible in $R[x]$.

Replace f by $f/\mathrm{cont}(f)$ to assume now that $\mathrm{cont}(f) = 1$. Factor f into irreducibles in $k[x]$ as

$$f = u \cdot p_1^{e_1} \cdots p_m^{e_m}$$

where u is in $k^\times$, the p_is are irreducibles in $k[x]$, and the e_is are positive integers. We can replace each p_i by $p_i/\mathrm{cont}(p_i)$ and replace u by

$$u \cdot \mathrm{cont}(p_1)^{e_1} \cdots \mathrm{cont}(p_m)^{e_m}$$

so then the new p_is are in $R[x]$ and have content 1. Since content is multiplicative, from $\mathrm{cont}(f) = 1$ we find that $\mathrm{cont}(u) = 1$, so u is a unit in R. The previous corollaries demonstrate the irreducibility of the (new) p_is in $R[x]$, so this gives a factorization of f into irreducibles in $R[x]$. That is, we have an explicit *existence* of a factorization into irreducibles.

Now suppose that we have two factorizations

$$f = u \cdot p_1^{e_1} \cdots p_m^{e_m} = v \cdot q_1^{f_1} \cdots q_n^{f_n}$$

where u, v are in R (and have unique factorizations there) and the p_i and q_j are irreducibles in $R[x]$ of positive degree. From above, all the contents of these irreducibles must be 1. Looking at this factorization in $k[x]$, it must be that $m = n$ and up to renumbering p_i differs from q_i by a constant in $k^\times$, and $e_i = f_i$. Since all these polynomials have content 1, in fact p_i differs from q_i by a unit in R. By equating the contents of both sides, we see that u and v differ by a unit in $R^\times$. Thus, by the unique factorization in R their factorizations into irreducibles in R (and, from above, in $R[x]$) must be essentially the same. Thus, we obtain uniqueness of factorization in $R[x]$. ///

3. *Worked examples*

[12.1] Let R be a principal ideal domain. Let I be a non-zero prime ideal in R. Show that I is *maximal*.

Suppose that I were strictly contained in an ideal J. Let $I = Rx$ and $J = Ry$, since R is a PID. Then x is a multiple of y, say $x = ry$. That is, $ry \in I$. But y is not in I (that is, not a multiple of p), since otherwise $Ry \subset Rx$. Thus, since I is prime, $r \in I$, say $r = ap$. Then $p = apy$, and (since R is a domain) $1 = ay$. That is, the ideal generated by y contains 1, so is the whole ring R. That is, I is maximal (proper).

[12.2] Let k be a field. Show that in the polynomial ring $k[x, y]$ in two variables the ideal $I = k[x, y] \cdot x + k[x, y] \cdot y$ is not principal.

Suppose that there were a polynomial $P(x, y)$ such that $x = g(x, y) \cdot P(x, y)$ for some polynomial g and $y = h(x, y) \cdot P(x, y)$ for some polynomial h.

An intuitively appealing thing to say is that since y *does not appear* in the polynomial x, it could not *appear* in $P(x, y)$ or $g(x, y)$. Similarly, since x *does not appear* in the polynomial y, it could not appear in $P(x, y)$ or $h(x, y)$. And, thus, $P(x, y)$ would be in k. It would have to be non-zero to yield x and y as multiples, so would be a unit in $k[x, y]$. Without loss of generality, $P(x, y) = 1$. (Thus, we need to show that I is proper.)

On the other hand, since $P(x, y)$ is supposedly in the ideal I generated by x and y, it is of the form $a(x, y) \cdot x + b(x, y) \cdot y$. Thus, we would have

$$1 = a(x, y) \cdot x + b(x, y) \cdot y$$

Mapping $x \longrightarrow 0$ and $y \longrightarrow 0$ (while mapping k to itself by the identity map, thus sending 1 to $1 \neq 0$), we would obtain

$$1 = 0$$

contradiction. Thus, there is no such $P(x, y)$.

We can be more precise about that admittedly intuitively appealing first part of the argument. That is, let's show that if

$$x = g(x, y) \cdot P(x, y)$$

then the degree of $P(x, y)$ (and of $g(x, y)$) as a polynomial in y (with coefficients in $k[x]$) is 0. Indeed, looking at this equality as an equality in $k(x)[y]$ (where $k(x)$ is the field of rational functions in x with coefficients in k), the fact that degrees *add* in products gives the desired conclusion. Thus,

$$P(x, y) \in k(x) \cap k[x, y] = k[x]$$

Similarly, $P(x, y)$ lies in $k[y]$, so P is in k.

[12.3] Let k be a field, and let $R = k[x_1, \ldots, x_n]$. Show that the inclusions of ideals

$$Rx_1 \subset Rx_1 + Rx_2 \subset \ldots \subset Rx_1 + \ldots + Rx_n$$

are *strict*, and that all these ideals are *prime.*

One approach, certainly correct in spirit, is to say that *obviously*

$$k[x_1, \ldots, x_n]/Rx_1 + \ldots + Rx_j \approx k[x_{j+1}, \ldots, x_n]$$

The latter ring is a domain (since k is a domain and polynomial rings over domains are domains: proof?) so the ideal was necessarily prime.

But while it is true that certainly $x_1, \ldots, x_j$ go to 0 in the quotient, our intuition uses the explicit construction of polynomials as *expressions* of a certain form. Instead, one might try to give the allegedly trivial and immediate proof that sending $x_1, \ldots, x_j$ to 0 does not somehow cause 1 to get mapped to 0 in k, nor accidentally impose any relations on $x_{j+1}, \ldots, x_n$. A too classical viewpoint does not lend itself to clarifying this. The point is that, given a k-algebra homomorphism $f_o : k \longrightarrow k$, here taken to be the *identity*, and given values 0 for $x_1, \ldots, x_j$ and values $x_{j+1}, \ldots, x_n$ respectively for the other indeterminates, there is a *unique* k-algebra homomorphism $f : k[x_1, \ldots, x_n] \longrightarrow k[x_{j+1}, \ldots, x_n]$ agreeing with f_o on k and sending $x_1, \ldots, x_n$ to their specified targets. Thus, in particular, we *can* guarantee that $1 \in k$ is *not* somehow accidentally mapped to 0, and no relations among the $x_{j+1} \ldots, x_n$ are mysteriously introduced.

[12.4] Let k be a field. Show that the ideal M generated by $x_1, \ldots, x_n$ in the polynomial ring $R = k[x_1, \ldots, x_n]$ is *maximal* (proper).

We prove the maximality by showing that R/M is a field. The universality of the polynomial algebra implies that, given a k-algebra homomorphism such as the *identity* $f_o : k \longrightarrow k$, and given $\alpha_i \in k$ (take $\alpha_i = 0$ here), there exists a unique k-algebra homomorphism $f : k[x_1, \ldots, x_n] \longrightarrow k$ extending f_o. The kernel of f certainly contains M, since M is generated by the x_i and all the x_i go to 0.

As in the previous exercise, one perhaps should verify that M is *proper*, since otherwise accidentally in the quotient map $R \longrightarrow R/M$ we might *not* have $1 \longrightarrow 1$. If we *do* know that M is a proper ideal, then by the uniqueness of the map f we know that $R \longrightarrow R/M$ is (up to isomorphism) exactly f, so M is maximal proper.

Given a relation

$$1 = \sum_i f_i \cdot x_i$$

with polynomials f_i, using the universal mapping property send all x_i to 0 by a k-algebra homomorphism to k that does send 1 to 1, obtaining $1 = 0$, contradiction.

[3.0.1] **Remark:** One surely is inclined to allege that *obviously* $R/M \approx k$. And, indeed, this quotient is *at most* k, but one should at least acknowledge *concern* that it not be accidentally 0. Making the point that not only can the images of the x_i be chosen, but *also* the k-algebra homomorphism on k, decisively eliminates this possibility.

[12.5] Show that the maximal ideals in $R = \mathbb{Z}[x]$ are all of the form

$$I = R \cdot p + R \cdot f(x)$$

where p is a prime and $f(x)$ is a monic polynomial which is irreducible modulo p.

Suppose that no non-zero integer n lies in the maximal ideal I in R. Then $\mathbb{Z}$ would inject to the quotient R/I, a field, which then would be of characteristic 0. Then R/I would contain a canonical copy of $\mathbb{Q}$. Let α be the image of x in K. Then $K = \mathbb{Z}[\alpha]$, so certainly $K = \mathbb{Q}[\alpha]$, so α is algebraic over $\mathbb{Q}$, say of degree n. Let $f(x) = a_n x^n + \ldots + a_1 x + a_0$ be a polynomial with rational coefficient such that $f(\alpha) = 0$, and with all denominators multiplied out to make the coefficients *integral*. Then let $\beta = c_n \alpha$: this β is still algebraic over $\mathbb{Q}$, so $\mathbb{Q}[\beta] = \mathbb{Q}(\beta)$, and certainly $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$, and $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$. Thus, we still have $K = \mathbb{Q}[\beta]$, but now things have been adjusted so that β satisfies a *monic* equation with coefficients in $\mathbb{Z}$: from

$$0 = f(\alpha) = f(\frac{\beta}{c_n}) = c_n^{1-n} \beta^n + c_{n-1} c_n^{1-n} \beta^{n-1} + \ldots + c_1 c_n^{-1} \beta + c_0$$

we multiply through by c_n^{n-1} to obtain

$$0 = \beta^n + c_{n-1} \beta^{n-1} + c_{n-2} c_n \beta^{n-2} + c_{n-3} c_n^2 \beta^{n-3} + \ldots + c_2 c_n^{n-3} \beta^2 + c_1 c_n^{n-2} \beta + c_0 c_n^{n-1}$$

Since $K = \mathbb{Q}[\beta]$ is an n-dimensional Q-vectorspace, we can find rational numbers b_i such that

$$\alpha = b_0 + b_1 \beta + b_2 \beta^2 + \ldots + b_{n-1} \beta^{n-1}$$

Let N be a large-enough integer such that for every index i we have $b_i \in \frac{1}{N} \cdot \mathbb{Z}$. Note that because we made β satisfy a *monic integer* equation, the set

$$\Lambda = \mathbb{Z} + \mathbb{Z} \cdot \beta + \mathbb{Z} \cdot \beta^2 + \ldots + \mathbb{Z} \cdot \beta^{n-1}$$

is closed under multiplication: β^n is a $\mathbb{Z}$-linear combination of lower powers of β, and so on. Thus, since $\alpha \in N^{-1} \Lambda$, successive powers α^ℓ of α are in $N^{-\ell} \Lambda$. Thus,

$$\mathbb{Z}[\alpha] \subset \bigcup_{\ell \geq 1} N^{-\ell} \Lambda$$

But now let p be a prime not dividing N. We claim that $1/p$ does not lie in $\mathbb{Z}[\alpha]$. Indeed, since $1, \beta, \ldots, \beta^{n-1}$ are linearly independent over $\mathbb{Q}$, there is a *unique* expression for $1/p$ as a $\mathbb{Q}$-linear combination of them, namely the obvious $\frac{1}{p} = \frac{1}{p} \cdot 1$. Thus, $1/p$ is not in $N^{-\ell} \cdot \Lambda$ for any $\ell \in \mathbb{Z}$. This (at last) contradicts the supposition that no non-zero integer lies in a maximal ideal I in $\mathbb{Z}[x]$.

Note that the previous argument uses the infinitude of primes.

Thus, $\mathbb{Z}$ does *not* inject to the field R/I, so R/I has positive characteristic p, and the canonical $\mathbb{Z}$-algebra homomorphism $\mathbb{Z} \longrightarrow R/I$ factors through $\mathbb{Z}/p$. Identifying $\mathbb{Z}[x]/p \approx (\mathbb{Z}/p)[x]$, and granting (as proven in an earlier homework solution) that for $J \subset I$ we can take a quotient in two stages

$$R/I \approx (R/J)/(\text{image of } J \text{ in } R/I)$$

Thus, the image of I in $(\mathbb{Z}/p)[x]$ is a maximal ideal. The ring $(\mathbb{Z}/p)[x]$ is a PID, since $\mathbb{Z}/p$ is a field, and by now we know that the maximal ideals in such a ring are of the form $\langle f \rangle$ where f is irreducible and of positive degree, and conversely. Let $F \in \mathbb{Z}[x]$ be a polynomial which, when we reduce its coefficients modulo p, becomes f. Then, at last,

$$I = \mathbb{Z}[x] \cdot p + \mathbb{Z}[x] \cdot f(x)$$

as claimed.

[12.6] Let R be a *PID*, and x, y non-zero elements of R. Let $M = R/\langle x \rangle$ and $N = R/\langle y \rangle$. Determine $\mathrm{Hom}_R(M, N)$.

Any homomorphism $f : M \longrightarrow N$ gives a homomorphism $F : R \longrightarrow N$ by composing with the quotient map $q : R \longrightarrow M$. Since R is a free R-module on one generator 1, a homomorphism $F : R \longrightarrow N$ is completely determined by $F(1)$, and this value can be anything in N. Thus, the homomorphisms from R to N are exactly parametrized by $F(1) \in N$. The remaining issue is to determine which of these maps F *factor through* M, that is, which such F admit $f : M \longrightarrow N$ such that $F = f \circ q$. We could *try* to define (and there is no other choice if it is to succeed)

$$f(r + Rx) = F(r)$$

but this will be well-defined if and only if $\ker F \supset Rx$.

Since $0 = y \cdot F(r) = F(yr)$, the kernel of $F : R \longrightarrow N$ invariably contains Ry, and we need it to contain Rx as well, for F to give a well-defined map $R/Rx \longrightarrow R/Ry$. This is equivalent to

$$\ker F \supset Rx + Ry = R \cdot \gcd(x, y)$$

or

$$F(\gcd(x, y)) = \{0\} \subset R/Ry = N$$

By the R-linearity,

$$R/Ry \ni 0 = F(\gcd(x, y)) = \gcd(x, y) \cdot F(1)$$

Thus, the condition for well-definedness is that

$$F(1) \in R \cdot \frac{y}{\gcd(x, y)} \subset R/Ry$$

Therefore, the desired homomorphisms f are in bijection with

$$F(1) \in R \cdot \frac{y}{\gcd(x, y)}/Ry \subset R/Ry$$

where

$$f(r + Rx) = F(r) = r \cdot F(1)$$

[12.7] *(A warm-up to Hensel's lemma)* Let p be an odd prime. Fix $a \not\equiv 0 \bmod p$ and suppose $x^2 = a \bmod p$ has a solution x_1. Show that for every positive integer n the congruence $x^2 = a \bmod p^n$ has a solution x_n. (*Hint:* Try $x_{n+1} = x_n + p^n y$ and solve for $y \bmod p$).

Induction, following the hint: Given x_n such that $x_n^2 = a \bmod p^n$, with $n \geq 1$ and $p \neq 2$, show that there will exist y such that $x_{n+1} = x_n + yp^n$ gives $x_{n+1}^2 = a \bmod p^{n+1}$. Indeed, expanding the desired equality, it is equivalent to

$$a = x_{n+1}^2 = x_n^2 + 2x_n p^n y + p^{2n} y^2 \bmod p^{n+1}$$

Since $n \geq 1$, $2n \geq n + 1$, so this is

$$a = x_n^2 + 2x_n p^n y \bmod p^{n+1}$$

Since $a - x_n^2 = k \cdot p^n$ for some integer k, dividing through by p^n gives an equivalent condition

$$k = 2x_n y \bmod p$$

Since $p \neq 2$, and since $x_n^2 = a \neq 0 \bmod p$, $2x_n$ is invertible mod p, so no matter what k is there exists y to meet this requirement, and we're done.

[12.8] *(Another warm-up to Hensel's lemma)* Let p be a prime not 3. Fix $a \neq 0 \bmod p$ and suppose $x^3 = a \bmod p$ has a solution x_1. Show that for every positive integer n the congruence $x^3 = a \bmod p^n$ has a solution x_n. (*Hint:* Try $x_{n+1} = x_n + p^n y$ and solve for y mod p.)

Induction, following the hint: Given x_n such that $x_n^3 = a \bmod p^n$, with $n \geq 1$ and $p \neq 3$, show that there will exist y such that $x_{n+1} = x_n + yp^n$ gives $x_{n+1}^3 = a \bmod p^{n+1}$. Indeed, expanding the desired equality, it is equivalent to

$$a = x_{n+1}^3 = x_n^3 + 3x_n^2 p^n y + 3x_n p^{2n} y^2 + p^{3n} y^3 \bmod p^{n+1}$$

Since $n \geq 1$, $3n \geq n+1$, so this is

$$a = x_n^3 + 3x_n^2 p^n y \bmod p^{n+1}$$

Since $a - x_n^3 = k \cdot p^n$ for some integer k, dividing through by p^n gives an equivalent condition

$$k = 3x_n^2 y \bmod p$$

Since $p \neq 3$, and since $x_n^3 = a \neq 0 \bmod p$, $3x_n^2$ is invertible mod p, so no matter what k is there exists y to meet this requirement, and we're done.

Exercises

12.[3.0.1] Let k be a field. Show that every non-zero prime ideal in $k[x]$ is maximal.

12.[3.0.2] Let k be a field. Let x, y, z be indeterminates. Show that the ideal I in $k[x, y, z]$ generated by x, y, z is not principal.

12.[3.0.3] Let R be a commutative ring with identity that is *not necessarily* an integral domain. Let S be a multiplicative subset of R. The localization $S^{-1}R$ is defined to be the set of pairs (r, s) with $r \in R$ and $s \in S$ modulo the equivalence relation

$$(r, s) \sim (r', s') \iff \text{there is } t \in S \text{ such that} t \cdot (rs' - r's) = 0$$

Show that the natural map $i_S : r \longrightarrow (r, 1)$ is a ring homomorphism, and that $S^{-1}R$ is a ring in which every element of S becomes invertible.

12.[3.0.4] Indeed, in the situation of the previous exercise, show that every ring homomorphism $\varphi : R \longrightarrow R'$ such that $\varphi(s)$ is invertible in R' for $s \in S$ *factors uniquely through* $S^{-1}R$. That is, there is a unique $f : S^{-1}R \longrightarrow R'$ such that $\varphi = f \circ i_S$ with the natural map i_S.