[08.1] 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).

[08.2] 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 $x \to 0$ and $y \to 0$ (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.

[08.3] 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 $f_o : k \to k$, 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 $f : k[x_1, \ldots, x_n] \to k[x_{j+1}, \ldots, x_n]$ 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.

[08.4] 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* $f_o : k \to k$, and given $\alpha_i \in k$ (take $\alpha_i = 0$ here), there exists a unique k-algebra homomorphism $f : k[x_1, \ldots, x_n] \to k$ 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 $R \to R/M$ we might *not* have $1 \to 1$. If we *do* know that M is a proper ideal, then by the uniqueness of the map f we know that $R \to R/M$ 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.

[0.0.1] **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.

[08.5] 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 $\mathbb{Z} \to R/I$ 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.

[08.6] 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 $f : M \to N$ gives a homomorphism $F : R \to N$ by composing with the quotient map $q : R \to M$. Since R is a free R-module on one generator 1, a homomorphism $F : R \to N$ 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 $f : M \to N$ 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 $F : R \to N$ invariably contains Ry, and we need it to contain Rx as well, for F to give a well-defined map $R/Rx \to R/Ry$. 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

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

[08.7] *(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.

[08.8] *(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 $y \bmod p$).]

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.