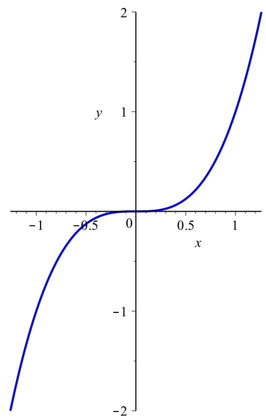
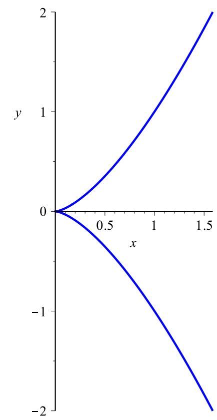
Math 662 — Homework 1

Spring 2014
Drew Armstrong

Problem 0 (Drawing Pictures). Sketch the curves $y^2 = f(x)$ in $\mathbb{R}^2$ for the following polynomials $f(x) \in \mathbb{R}[x]$: $f(x) = x^3$ and $f(x) = (x+1)(x^2+\varepsilon)$ for $\varepsilon < 0$, $\varepsilon = 0$, $\varepsilon > 0$. [Hint: First sketch $y = f(x)$ then sketch $y = \pm\sqrt{f(x)}$.]

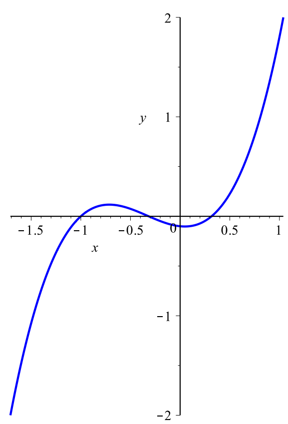
The curves $y = x^3$ and $y^2 = x^3$ look like:

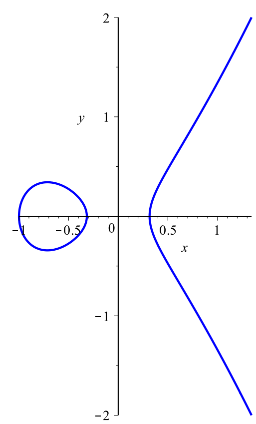




Note that the curve on the right has a "cusp" at $x = 0$ because the derivative $\frac{dy}{dx} = \pm\frac{3}{2}\sqrt{x}$ approaches 0 as $x \to 0$ from the right.

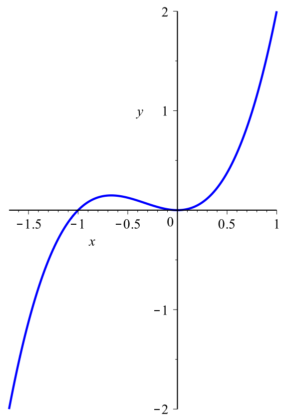
The curves $y = (x+1)(x^2+\varepsilon)$ and $y = (x+1)(x^2+\varepsilon)$ for $\varepsilon < 0$ look like:

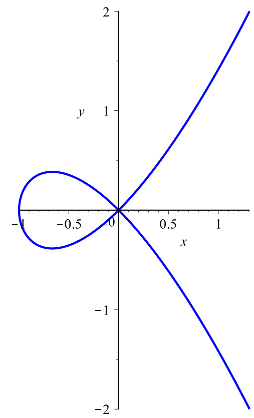




Note that the three roots of $f(x)$ are simple, and so the graph looks locally like a straight line $y = \alpha x$ at one of these points. Then the graph of $y^2 = f(x)$ looks locally like $\pm\sqrt{\alpha x}$, i.e., a parabola opening to the side. Note: Near $\varepsilon = -1$ the blob on the right shrinks to a single point at $(x, y) = (-1, 0)$. Why?

For $\varepsilon = 0$, the curves $y = x^2(x+1)$ and $y^2 = x^2(x+1)$ look like:



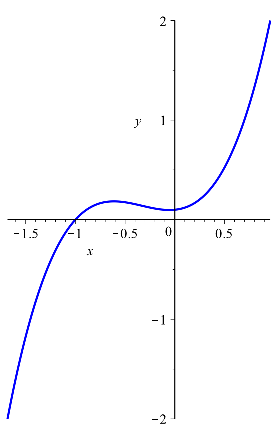


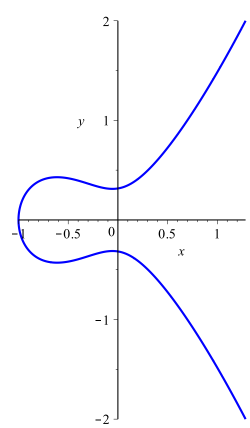
As discussed, since $f(x)$ has a simple root at $x = -1$, the graph of $\pm\sqrt{f(x)}$ has a vertical tangent at $x = -1$. What's going on at $x = 0$? Near $x = 0$, Newton's binomial theorem tells us that

$$\pm\sqrt{1+x} = \pm\left(1 + \frac{(1/2)}{1!}x + \frac{(1/2)(-1/2)}{2!}x^2 + \frac{(1/2)(-1/2)(-3/2)}{3!}x^3 + \cdots\right)$$

Thus the graph of $y = \pm\sqrt{x^2(x+1)} = \pm x\sqrt{1+x}$ looks locally like the union of the two lines $y = \pm x$. We say that the curve has two "branches" at the "node" $(x, y) = (0, 0)$.

The curves $y = (x+1)(x^2+\varepsilon)$ and $y^2 = (x+1)(x^2+\varepsilon)$ for $\varepsilon > 0$ look like:

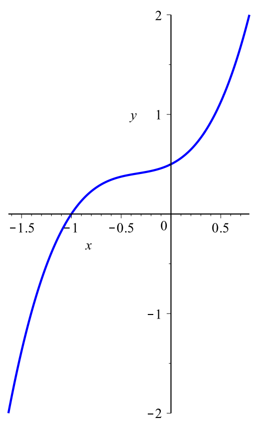


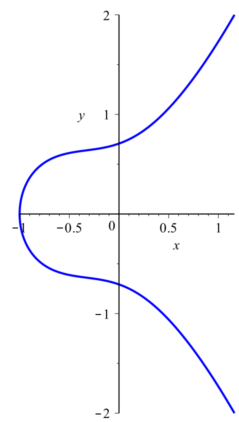


Again, the graph of $y = \pm\sqrt{f(x)}$ has a vertical tangent at $x = -1$ because $f(x)$ has a simple root there. For values $0 < \varepsilon < 1/3$ (as pictured) there will be local extrema at

$$x = \frac{-1 \pm \sqrt{1-3\varepsilon}}{3}$$

but for values $\varepsilon > 1/3$ these extrema will go away. In that case the curves $y = (x+1)(x^2+\varepsilon)$ and $y^2 = (x+1)(x^2+\varepsilon)$ will look like:





[Now you have a mental picture of plane cubic curves. These were first classified by Isaac Newton in 1695. In fact, any curve of the form $f(x,y) = 0$ where $f(x,y) \in \mathbb{R}[x,y]$ has degree 3 is equivalent to one of the curves seen above. To be precise we will need to introduce projective coordinates. Stay tuned.]

What is a polynomial? Let R be a ring and let x be a formal symbol. A polynomial is a formal expression $a_0 + a_1x^1 + a_2x^2 + \cdots$ in which all but finitely many of the coefficients $a_i \in R$ are zero. If we define addition and multiplication by

$$\sum_k a_k x^k + \sum_k b_k x^k := \sum_k (a_k + b_k) x^k$$

and

$$\left(\sum_k a_k x^k\right)\left(\sum_\ell b_\ell x^\ell\right) := \sum_m \left(\sum_{k+\ell=m} a_k b_\ell\right) x^m,$$

then the set of polynomials becomes a ring which we call $R[x]$. Note that R is naturally embedded in $R[x]$ as a subring via the map $a \mapsto a + 0x + 0x^2 + \cdots$. We define the degree $\deg(f)$ of a nonzero polynomial $f(x) = \sum_k a_k x^k$ as the largest k such that $a_k \neq 0$ (this a_k is called the leading coefficient), and we define the degree of the zero polynomial as $\deg(0) = -\infty$ (but this is rather arbitrary). We consider the symbols $1, x, x^2, \ldots$ to be linearly independent over R, and therefore we have $\sum_k a_k x^k = \sum_k b_k x^k$ if and only if $a_k = b_k$ for all k. This makes $R[x]$ into an infinite-dimensional "free" module over R.

Problem 1 (The Division Algorithm). We say that a polynomial $g(x) \in R[x]$ is monic if its leading coefficient is a unit. Consider polynomials $f(x) = \sum_k a_k x^k$ and $g(x) = \sum_k b_k x^k$ in $R[x]$ with $g(x)$ monic.

(a) Prove that **there exist** polynomials $q(x), r(x) \in R[x]$ such that $f(x) = q(x)g(x) + r(x)$ and $\deg(r) < \deg(g)$ (this includes the case $r(x) = 0$ since $\deg(0) = -\infty < \deg(g)$ for any g). [Hint: Use induction on $\deg(f)$. Assume that $\deg(g) = m \geq 0$ with leading coefficient $b_m \in R^\times$. If $\deg(f) < m$ then we can take $q(x) = 0$ and $r(x) = f(x)$, so the assertion is true. Now suppose that $\deg(f) = n \geq m$ and consider the polynomial $f_1(x) = f(x) - \frac{a_n}{b_m}x^{n-m}g(x)$. Since $\deg(f_1) < n$ there exist $q_1(x), r(x)$ with $f_1(x) = q_1(x)g(x) + r(x)$ and $\deg(r) < \deg(g)$.]

(b) Prove that the polynomials $q(x), r(x)$ from part (a) are **unique**. [Hint: Assume that $f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$ with $\deg(r_1), \deg(r_2) < \deg(g)$. Since $g(x)$ is monic, note that $\deg(gh) = \deg(g) + \deg(h)$ for any nonzero $h(x) \in R[x]$. Note that $\deg(r_2 - r_1) \leq \max\{\deg(r_1), \deg(r_2)\}$. Now assume that $r_2(x) - r_1(x) \neq 0$ and show that this leads to a contradiction.]

(c) Give an example where $g(x)$ is not monic and the polynomials $q(x), r(x)$ do not exist.

Proof. Let R be any ring and consider $f(x), g(x) \in R[x]$ with $g(x)$ monic. Let $g(x) = b_0 + b_1x + \cdots + b_mx^m$ where $b_m \in R^\times$ is a unit, hence $\deg(g) = m \geq 0$. We will show by induction on $\deg(f)$ that there exist $q(x), r(x) \in R[x]$ with $f(x) = q(x)g(x) + r(x)$ and $\deg(r) < m$. First note that the result is true if $\deg(f) < m$, in which case we can take $q(x) = 0$ and $r(x) = f(x)$. So suppose that $\deg(f) = n \geq m$. Since b_m is a unit we can define the polynomial $f_1(x) = f(x) - \frac{a_n}{b_m}x^{n-m}g(x)$. Note that $\deg(f_1) < \deg(f)$ so by induction there exist $q_1(x), r(x) \in R[x]$ with $f_1(x) = q_1(x)g(x) + r(x)$ and $\deg(r) < \deg(g)$. Finally, we have

$$\begin{aligned} f(x) &= f_1(x) + \frac{a_n}{b_m}x^{n-m}g(x) \\ &= q_1(x)g(x) + r(x) + \frac{a_n}{b_m}x^{n-m}g(x) \\ &= \left(q_1(x) + \frac{a_n}{b_m}x^{n-m}\right)g(x) + r(x), \end{aligned}$$

where $\deg(r) < \deg(g)$, as desired.

To show that the quotient and remainder are unique, suppose we have

$$q_1(x)g(x) + r_1(x) = f(x) = q_2(x)g(x) + r_2(x)$$

with $\deg(r_1), \deg(r_2) < \deg(g)$. Rearranging the equations gives

$$(\star) \qquad g(x)\left(q_1(x) - q_2(x)\right) = \left(r_2(x) - r_1(x)\right).$$

Now assume for contradiction that $r_2(x) - r_1(x) \neq 0$. This implies that

$$0 \leq \deg(r_2 - r_1) \leq \max\{\deg(r_1), \deg(r_2)\} < \deg(g).$$

On the other hand, since $g(x)$ is monic we have $\deg(gh) = \deg(g) + \deg(h)$ for all $h(x) \in R[x]$. Since $q_1(x) - q_2(x) \neq 0$ this implies in particular that

$$\deg(g(q_1 - q_2)) = \deg(g) + \deg(q_1 - q_2) \geq \deg(g).$$

But this contradicts the equation $(\star)$. We conclude that $r_2(x) - r_1(x) = 0$, and hence $r_1(x) = r_2(x)$. Finally, since $g(x)\left(q_1(x) - q_2(x)\right) = 0$ and $g(x)$ is monic, we conclude that $q_1(x) - q_2(x) = 0$, and hence $q_1(x) = q_2(x)$.

Note that the existence and uniqueness of $q(x)$ and $r(x)$ can fail when $g(x)$ is not monic. For example, consider $f(x) = x^2 + x + 1$ and $g(x) = 2x + 2$ in $\mathbb{Z}/(6)[x]$. Then the quotient and remainder do **not exist**. (If we had $f(x) = q(x)g(x) + r(x)$ with $\deg(r) < \deg(g)$ then the leading coefficient a of $q(x)$ would satisfy $2a = 1$. But then $0 = 3(2a) = 3$. Contradiction.) If we change $f(x)$ to $4x^2 + 4x + 1$ then the quotient and remainder exist, but they are **not unique**:

$$(2x)(2x^2 + 2x) + 1 = 4x^2 + 4x + 1 = (5x)(2x^2 + 2x) + 1.$$

□

[By uniqueness we can speak of "the" remainder when $f(x)$ is divided by monic $g(x)$. We will write $g|f$ (and say "g divides f") if and only if the remainder is zero.]

Problem 2 (Descartes' Theorem). Let R be a ring (i.e. commutative).

(a) If $\alpha \in R$ is any element, we define a function $\mathsf{ev}_\alpha : R[x] \to R$ by sending $\sum_k a_k x^k \in R[x]$ to $\sum_k a_k \alpha^k \in R$. Prove that this function (called "evaluation at α") is a morphism of rings. For simplicity we will write $f(\alpha) := \mathsf{ev}_\alpha(f(x))$.

(b) Consider a polynomial $f(x) \in R[x]$ and an element $\alpha \in R$. Prove that we have $(x-\alpha)|f(x)$ if and only if $f(\alpha) = 0$. [Hint: Divide $f(x)$ by $(x-\alpha)$ and evaluate at α.]

Proof. First we show that $\mathsf{ev}_\alpha : R[x] \to R$ is a homomorphism of rings. Given $f(x) = \sum_k a_k x^k$ and $g(x) = \sum_k b_k x^k$ we have

$$\begin{aligned}(f+g)(\alpha) &= \sum_k (a_k + b_k)\alpha^k \\ &= \sum_k a_k \alpha^k + \sum_k b_k \alpha^k \\ &= f(\alpha) + g(\alpha)\end{aligned}$$

and

$$\begin{aligned}(fg)(\alpha) &= \sum_m \left(\sum_{k+\ell=m} a_k b_\ell \right) \alpha^m \\ &= \left(\sum_k a_k \alpha^k \right) \left(\sum_\ell b_\ell \alpha^\ell \right) \\ &= f(\alpha) g(\alpha).\end{aligned}$$

Finally, note that the unit polynomial $1 + 0x + 0x^2 + \cdots$ evalutes to $1 \in R$.

Now consider any $f(x) \in R[x]$ and $\alpha \in R$. Since $(x-\alpha)$ is monic, Problem 1 says that there exist a unique polynomial $q(x) \in R[x]$ and a constant $c \in R$ such that

$$f(x) = (x-\alpha)q(x) + c.$$

By definition we have $(x-\alpha)|f(x)$ if and only if $c = 0$. But part (a) tells us that $f(\alpha) = (\alpha - \alpha)q(\alpha) + c = 0 \cdot q(\alpha) + c = c$. □

[The importance of Descartes' Theorem cannot be overestimated.]

Problem 3 (Localization of a Ring). The construction of the field of fractions of a domain can be generalized to arbitrary rings as follows. Let R be a ring and let $S \subseteq R$ be any subset closed under multiplication and containing 1 (we can say that S is a subsemigroup of $(R, \times, 1)$). We define the set of formal symbols

$$R[S^{-1}] := \left\{ \left[\frac{a}{b} \right] : a, b \in R, b \in S \right\}$$

and we declare that

$$\left[\frac{a}{b} \right] = \left[\frac{c}{d} \right] \Longleftrightarrow \exists\, u \in S \text{ such that } u(ad - bc) = 0.$$

(a) Prove that this is an equivalence relation.

(b) Prove that the algebraic operations

$$\left[\frac{a}{b}\right]\left[\frac{c}{d}\right] := \left[\frac{ac}{bd}\right]$$

and

$$\left[\frac{a}{b}\right]+\left[\frac{c}{d}\right] := \left[\frac{ad+bc}{bd}\right]$$

are well-defined. It follows (don't prove this) that $R[S^{-1}]$ is a ring.

(c) Prove that $R[S^{-1}] = 0$ if and only if S contains 0.

(d) Prove that the natural map $R \to R[S^{-1}]$ defined by $a \mapsto \left[\frac{a}{1}\right]$ is a ring homomorphism.

(e) We say that $u \in R$ is a zerodivisor if there exists $v \in R$ such that $uv = 0$. If S contains no zerodivisors, prove that the natural map $R \to R[S^{-1}]$ is injective. (This holds in particular when R is a domain and $0 \notin S$.)

(f) If $P \subseteq R$ is a prime ideal, show that $S := R - P$ is a subsemigroup of R. The localization $R[S^{-1}]$ is denoted as R_P and is called the localization of R at the prime P. We will discuss the geometric meaning of this later.

Proof. For part (a), consider any $a, b \in R$ with $b \in S$. Since $1(ab - ba) = 0$ and $1 \in S$ we have $\left[\frac{a}{b}\right] = \left[\frac{a}{b}\right]$. Next, consider $a, b, c, d \in R$ with $b, d \in S$ such that $\left[\frac{a}{b}\right] = \left[\frac{c}{d}\right]$, i.e., there exists $u \in S$ such that $u(ad - bc) = 0$. But then $u(cb - da) = -0 = 0$, hence $\left[\frac{c}{d}\right] = \left[\frac{a}{b}\right]$. Finally, assume that $\left[\frac{a}{b}\right] = \left[\frac{c}{d}\right]$ and $\left[\frac{c}{d}\right] = \left[\frac{e}{f}\right]$, i.e., there exist $u, v \in S$ such that $u(ad - bc) = 0$ and $v(cf - de) = 0$. Then we have

$$\begin{aligned} duv(af) &= (uad)vf, \\ &= (ubc)vf, \\ &= (vcf)ub, \\ &= (vde)ub, \\ &= duv(be). \end{aligned}$$

Since $d, u, v \in S$ we have $duv \in S$ and hence $\left[\frac{a}{b}\right] = \left[\frac{e}{f}\right]$.

For part (b) assume that $\left[\frac{a}{b}\right] = \left[\frac{a'}{b'}\right]$ and $\left[\frac{c}{d}\right] = \left[\frac{c'}{d'}\right]$, i.e., assume that we have $u(ab' - a'b) = 0$ and $v(cd' - c'd) = 0$ for some $u, v \in S$. Then we have

$$\begin{aligned} uv(acb'd') &= (uab')(vcd'), \\ &= (ua'b)(vc'd), \\ &= uv(a'c'bd). \end{aligned}$$

Since $u, v \in S$ we have $uv \in S$, and hence $\left[\frac{ac}{bd}\right] = \left[\frac{a'c'}{b'd'}\right]$. We also have

$$\begin{aligned} uv[(ad+bc)b'd'] &= uvadb'd' + uvbcb'd', \\ &= (uab')vdd' + (vcd')ubb', \\ &= (ua'b)vdd' + (vc'd)ubb', \\ &= uva'd'bd + uvb'c'bd, \\ &= uv[(a'd' + b'c')bd], \end{aligned}$$

and hence $\left[\frac{ad+bc}{bd}\right] = \left[\frac{a'd'+b'c'}{b'd'}\right]$. We will not bother to check that these operations define a ring structure on $R[S^{-1}]$. Is it possible that no one has ever checked this? Oh well.

For part (c), first assume that $0 \in S$. Then for all $a, b, c, d \in R$ with $b, d \in S$ we have $0(ad - bc) = 0$, and hence $\left[\frac{a}{b}\right] = \left[\frac{c}{d}\right]$. We conclude that $R[S^{-1}]$ consists of just one element, which we might as well call 0. Conversely, assume that $R[S^{-1}]$ consists of just one element. In particular, we have $\left[\frac{1}{1}\right] = \left[\frac{0}{1}\right]$. But this means that there exists $u \in S$ such that $u = u(1) = u(1 \cdot 1 - 1 \cdot 0) = 0$. We conclude that $0 \in S$.

For part (d), first note that $\left[\frac{1}{1}\right]$ is the unity in $R[S^{-1}]$, hence $1_R \mapsto 1_{R[S^{-1}]}$ as desired. Then, for any $a, b \in R$ we have

$$\left[\frac{a}{1}\right]\left[\frac{b}{1}\right] = \left[\frac{ab}{1 \cdot 1}\right] = \left[\frac{ab}{1}\right] \quad \text{and} \quad \left[\frac{a}{1}\right] + \left[\frac{b}{1}\right] = \left[\frac{a \cdot 1 + 1 \cdot b}{1}\right] = \left[\frac{a+b}{1}\right],$$

as desired.

For part (e), assume that R has no zerodivisors. We wish to show that the map $a \mapsto \left[\frac{a}{1}\right]$ is injective. So consider $a, b \in R$ and assume that $\left[\frac{a}{1}\right] = \left[\frac{b}{1}\right]$, i.e., there exists $u \in S$ such that $u(a - b) = 0$. Since u is not a zerodivisor, this implies that $a - b = 0$, hence $a = b$. I should have asked you to prove the converse statement: If the map $R \to R[S^{-1}]$ is an injection, then S contains no zerodivisors. I'll include the proof anyway. Assume that the map $a \mapsto \left[\frac{a}{1}\right]$ is injective and suppose that S contains a zerodivisor $u \in S$. That is, suppose that there exists $v \neq 0$ such that $uv = 0$. But then we have $1 + v \neq 1$ and $u(1 + v - 1) = 0$, hence $\left[\frac{1+v}{1}\right] = \left[\frac{1}{1}\right]$. This contradicts injectivity.

Finally, for part (f), let $P \leq R$ be a prime ideal. By definition this means that for all $a, b \in R$ we have

$$ab \in P \Longrightarrow a \in P \text{ or } b \in P.$$

If we let $S := R - P$ then the contrapositive of the above statement says that for all $a, b \in R$ we have

$$a \in S \text{ and } b \in S \Longrightarrow ab \in S.$$

Since $1 \in S$ (let's say that $P \neq R$ is part of the definition of "prime"), we conclude that S is a subsemigroup of $(R, \times, 1)$. As we will see later, the localization $R_P := R[S^{-1}]$ "at the prime P" is the most important example of localization. □

Problem 4 (Localization of $\mathbb{Z}$).

(a) Let $p \in \mathbb{Z}$ be prime and consider the localization $\mathbb{Z}_{(p)}$ at the prime ideal (p):

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b \right\}.$$

Prove that this ring has a unique nontrivial **maximal** ideal. [Hint: What are the units of $\mathbb{Z}_{(p)}$? Recall that an ideal is the whole ring if and only if it contains a unit.] A ring with a unique nontrivial maximal ideal is called a local ring.

(b) Prove that every ring $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$ between $\mathbb{Z}$ and $\mathbb{Q}$ is a localization of $\mathbb{Z}$. [Hint: Since R is a subring of $\mathbb{Q}$ it consists of fractions. Let S be the set of denominators that occur in elements of R. Prove that $R = \mathbb{Z}[S^{-1}]$.]

Proof. First we show (a). Since $\mathbb{Z}$ is a domain, the localization map $\mathbb{Z} \to \mathbb{Z}_{(p)}$ is an injection, thus (by slight abuse) we can regard $p \in \mathbb{Z}$ as an element of $\mathbb{Z}_{(p)}$. Now consider the principal ideal generated by p:

$$p\mathbb{Z}_{(p)} := \left\{ \frac{pa}{b} : a, b \in \mathbb{Z}, p \nmid b \right\}.$$

Note that this is not the unit ideal (i.e. $p\mathbb{Z}_{(p)} \neq \mathbb{Z}_{(p)}$) because it contains no units. Indeed, if $\frac{pa}{b}$ is in $p\mathbb{Z}_{(p)}$ then its inverse $\frac{b}{pa}$ is not in $\mathbb{Z}_{(p)}$ because it has p in the denominator. I claim that $p\mathbb{Z}_{(p)}$ is maximal and that it is the **only** maximal ideal of $\mathbb{Z}_{(p)}$. Indeed, let $I \leq \mathbb{Z}_{(p)}$ be any other ideal not contained in $p\mathbb{Z}_{(p)}$. Then there exists an element $\frac{a}{b} \in I - p\mathbb{Z}_{(p)}$, i.e., such that $p \nmid a$ and $p \nmid b$. But then $\frac{a}{b}$ is a unit with inverse $\frac{b}{a} \in \mathbb{Z}_{(p)}$ and it follows that $I = \mathbb{Z}_{(p)}$. We conclude that all nontrivial ideals of $\mathbb{Z}_{(p)}$ are contained in $p\mathbb{Z}_{(p)}$. It follows that $p\mathbb{Z}_{(p)}$ is the unique maximal ideal.

Now we show (b). Consider any ring $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$ between $\mathbb{Z}$ and $\mathbb{Q}$. Since R is a subring of $\mathbb{Q}$ it consists of fractions. Define

$$S := \left\{ b \in \mathbb{Z} : \frac{a}{b} \in R \text{ with } \gcd(a,b) = 1 \right\}.$$

(Note that the coprime condition is necessary, otherwise we have $\frac{b}{b} \in R$ and hence $b \in S$ for all nonzero b. That's no good.) I claim that $R = \mathbb{Z}[S^{-1}]$. Indeed, note that $R \subseteq \mathbb{Z}[S^{-1}]$ because every element of R has a denominator in the set S. Conversely, consider any $\frac{a}{b} \in \mathbb{Z}[S^{-1}]$; i.e., with $b \in S$. By definition of S there exists some $c \in \mathbb{Z}$ with $\frac{c}{b} \in R$ and $\gcd(c,d) = 1$. Then by Bézout's Lemma there exist $x, y \in \mathbb{Z}$ such that $cx + by = 1$. Dividing both sides by b gives

$$\frac{c}{b}x + y = \frac{1}{b}.$$

Since $\mathbb{Z} \subseteq R$ and $\frac{c}{b} \in R$ we conclude that $\frac{1}{b} \in R$. Finally, we conclude that $\frac{a}{b} = a\frac{1}{b} \in R$, and hence $\mathbb{Z}[S^{-1}] \subseteq R$. □

[More generally, let D be any domain in which Bézout's Lemma holds (for example, a PID). Then every intermediate ring $D \subseteq R \subseteq \mathrm{Frac}(D)$ is a localization of D. The proof is the same.]