The Hierarchy of Domains

Dylan C. Beck

Recall that a ring R is an abelian group $(R, +)$ with an associative and distributive multiplication $\cdot$ such that there exists a unique element 1_R that satisfies $r \cdot 1_R = r = 1_R \cdot r$ for every element r of R. Further, we say that a ring R is **commutative** whenever we have that $rs \stackrel{\text{def}}{=} r \cdot s = s \cdot r \stackrel{\text{def}}{=} sr$ for all elements $r, s \in R$. We say that an element r of a commutative ring R is **regular** whenever $rs = 0_R$ implies that $s = 0_R$. Given that every nonzero element r of a commutative ring R is regular, we say that R is an **integral domain**. We say that an element r of R is a **unit** whenever there exists a unique element r^{-1} of R such that $rr^{-1} = 1_R = r^{-1}r$. Given that every nonzero element r of a commutative ring R is a unit, we say that R is a **field**. Previously, we established that a field is an integral domain; however, there exist integral domains that are not fields, e.g., the integers $\mathbb{Z}$. Our aim throughout this note is to understand to what extent an integral domain fails to be a field.

Given a rng R, we may define the collection of univariate polynomials over R by

$$R[x] = \{r_n x^n + \cdots + r_1 x + r_0 \,|\, n \geq 0 \text{ is an integer and } r_0, r_1, \ldots, r_n \in R\}.$$

One can prove that $R[x]$ is a rng (with respect to the usual polynomial addition and multiplication) that inherits many of the properties of R. For instance, it is straightforward to show that if R is a ring (i.e., if R possesses a multiplicative identity 1_R), then $R[x]$ is a ring, and if R is commutative, then $R[x]$ is commutative. We will need the following two propositions for later discussion.

Proposition 1. We have that R is an integral domain if and only if $R[x]$ is an integral domain.

Proof. If $R[x]$ is an integral domain, then R is an integral domain, as R is a subring of $R[x]$. (Why?) Conversely, we will assume that R is an integral domain. Given any two nonzero polynomials $f(x) = r_m x^m + \cdots + r_1 x + r_0$ and $g(x) = s_n x^n + \cdots + s_1 x + s_0$ of $R[x]$, we may assume that r_m and s_n are nonzero (otherwise, we may take r_m and s_n to be the largest nonzero coefficients of $f(x)$ and $g(x)$, respectively). Observe that $f(x)g(x) = r_m s_n x^{m+n} + \text{lower order terms}$. By hypothesis that R is a domain with r_m and s_n nonzero, it follows that $r_m s_n$ is nonzero so that $f(x)g(x)$ is a nonzero polynomial. Consequently, every nonzero element of $R[x]$ is regular, hence $R[x]$ is a domain. □

Proposition 2. Let R be an integral domain (so that $R[x]$ is an integral domain by Proposition 1). We have that u is a unit of $R[x]$ if and only if u is a unit of R.

Proof. Certainly, if u is a unit of R, then the constant polynomial u is a unit of $R[x]$. Conversely, we will assume that $u = r_n x^n + \cdots + r_1 x + r_0$ is a unit of $R[x]$. Consequently, there exist elements $s_0, s_1, \ldots, s_m$ of R such that $u^{-1} = s_m x^m + \cdots + s_1 x + s_0$ and $1_R = uu^{-1}$. By hypothesis that R is an integral domain, we must have that $0 = \deg 1_R = \deg(uu^{-1}) = \deg u + \deg u^{-1}$ so that u and u^{-1} are constant. We conclude that $u = r_0$ and $u^{-1} = s_0$ with $1_R = r_0 s_0$, i.e., u is a unit of R. □

Euclidean Domains

Our prototypical example of an integral domain that is not a field is the ring of integers $\mathbb{Z}$. Observe that the only units in $\mathbb{Z}$ are ± 1: indeed, we have that $n \cdot \frac{1}{n} = 1$, hence if the integer n is a unit, then its unique multiplicative inverse $\frac{1}{n}$ is an integer. Consequently, we must have that $n = \pm 1$.

Given any integers a and $b \neq 0$, the Euclidean Algorithm (or the Division Algorithm) guarantees that there exist unique integers q and r such that $0 \leq |r| < |b|$ and $a = bq + r$. We refer to the integer q as the **quotient** and the integer r as the **remainder**. Even more, for any two nonzero integers a and b, we have that $|a| \leq |a||b| = |ab|$. Consequently, we refer to the absolute value function $|\cdot| : \mathbb{Z} \to \mathbb{Z}_{\geq 0}$ as a (multiplicative) **Euclidean function**. Generally, a Euclidean function (or **valuation**) on an integral domain R is a map $\upsilon : R \setminus \{0_R\} \to \mathbb{Z}_{\geq 0}$ that satisfies

(i.) the Euclidean Algorithm, i.e., for any element a and any nonzero element b of R, there exist some elements q and r of R such that $a = bq + r$ and either $r = 0_R$ or $\upsilon(r) < \upsilon(b)$ and

(ii.) for all nonzero elements a and b of R, we have that $\upsilon(a) \leq \upsilon(ab)$.

We say that a valuation υ is **multiplicative** whenever $\upsilon(a) \geq 1$ and $\upsilon(ab) = \upsilon(a)\upsilon(b)$. Given an integral domain R with a valuation $\upsilon : R \setminus \{0_R\} \to \mathbb{Z}_{\geq 0}$, we say that R is a **Euclidean domain**.

Proposition 3. Let R be a Euclidean domain with a multiplicative valuation $\upsilon : R \setminus \{0_R\} \to \mathbb{Z}_{\geq 0}$.

(a.) We have that $\upsilon(1_R) = 1$.

(b.) We have that $\upsilon(a) = 1$ if and only if a is a unit.

Proof. (a.) Observe that $\upsilon(1_R) = \upsilon(1_R \cdot 1_R) = \upsilon(1_R)\upsilon(1_R)$ implies that $\upsilon(1_R) = 1$. Explicitly, as $\mathbb{Z}$ is an integral domain, it follows from the identity $0 = \upsilon(1_R)\upsilon(1_R) - \upsilon(1_R) = \upsilon(1_R)(\upsilon(1_R) - 1)$ that $\upsilon(1_R) = 0$ or $\upsilon(1_R) = 1$. But the former is impossible because υ is multiplicative.

(b.) We will assume first that $\upsilon(a) = 1$. By hypothesis that υ is a valuation, there exist elements q and r of R such that $1_R = aq + r$ and either $r = 0_R$ or $\upsilon(r) < \upsilon(a) = 1$. Considering that υ is a multiplicative valuation, we must have that $\upsilon(r) \geq 1$, hence it is not possible that $\upsilon(r) < \upsilon(a) = 1$. We conclude therefore that $r = 0_R$ so that $1_R = aq$. Put another way, a is a unit. Conversely, if a is a unit, then we have that $1 = \upsilon(1_R) = \upsilon(aa^{-1}) = \upsilon(a)\upsilon(a^{-1})$ so that $\upsilon(a) = \upsilon(a^{-1}) = 1$. □

Example 1. Given a field k, consider the map $\upsilon : k \setminus \{0_k\} \to \mathbb{Z}_{\geq 0}$ defined by $\upsilon(x) = 1$. We leave it as an exercise to establish that υ is a (multiplicative) valuation, hence k is a Euclidean domain.

Example 2. Consider the subset $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$ of the complex numbers $\mathbb{C}$. Considering that $\mathbb{C}$ is a field (in the obvious way), we may show that $\mathbb{Z}[i]$ is a ring via the subring test. Evidently, $\mathbb{Z}[i]$ is closed under addition and multiplication and $1 = 1 + 0i$ is in $\mathbb{Z}[i]$, so we are done. We refer to the domain $\mathbb{Z}[i]$ as the **Gaussian integers**. One can show that the map $\upsilon : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ defined by $\upsilon(a + bi) = a^2 + b^2$ is a (multiplicative) valuation, hence $\mathbb{Z}[i]$ is a Euclidean domain.

Before we move to the next example, it is important to note that the Gaussian integers exhibit many interesting properties. One of the most extensive resources for studying the Gaussian integers is this blurb by Keith Conrad. We record the most useful facts about $\mathbb{Z}[i]$ in the following propositions.

Proposition 4. (Theorem 6.3 of Conrad) Consider the Gaussian integer $a+bi$. Given that a^2+b^2 is prime (as an integer), then $(a+bi)$ is a prime ideal of $\mathbb{Z}[i]$ (so that $a+bi$ is prime in $\mathbb{Z}[i]$).

Proposition 5. (Theorem 9.9 of Conrad) A prime element in $\mathbb{Z}[i]$ must be a unit multiple of

(a.) $1+i$; or

(b.) $a+bi$ or $a-bi$ such that a^2+b^2 is prime in $\mathbb{Z}$ and $a^2+b^2 \equiv 1 \pmod 4$; or

(c.) $p+0i$ such that p is prime in $\mathbb{Z}$ and $p \equiv 3 \pmod 4$.

Q2, August 2011. Find with proof the number of distinct ideals of the quotient ring $\mathbb{Z}[i]/6\mathbb{Z}[i]$.

Example 3. Given a field k, the polynomial ring $k[x]$ is a Euclidean domain. Consider the map $\upsilon : k[x] \setminus \{0_k\} \to \mathbb{Z}_{\geq 0}$ defined by $\upsilon(a_n x^n + \cdots + a_1 x + a_0) = \max\{i \,|\, a_i \neq 0\}$, i.e., $\upsilon(p(x))$ is the **degree** of $p(x)$. Using polynomial long division, we find that property (i.) of a valuation is satisfied by υ. Likewise, it is not difficult to see that property (ii.) of a valuation is satisfied for υ.

One of the fundamental properties of a Euclidean domain is that all of its ideals are principal.

Proposition 6. Let R be a Euclidean domain with a valuation υ. Given an ideal I of R, there exists an element x of I such that $I = xR$. Consequently, every ideal of R is principal.

Proof. Certainly, if I is the zero ideal, then we have that $I = 0_R R$. Consequently, we may assume that I is nonzero. Consider the set $V = \{\upsilon(i) \,|\, i \in I \text{ is nonzero}\} \subseteq \mathbb{Z}_{\geq 0}$. By the Well-Ordering Principle, there exists a minimal element $\upsilon(x)$ of V. We claim that $I = xR$. By hypothesis that I is an ideal and x is in I, we have that xr is in I for all elements r of R so that $xR \subseteq I$. Conversely, for any element y of I, there exist elements q and r of R such that $y = qx + r$ and either $r = 0_R$ or $\upsilon(r) < \upsilon(x)$. By assumption that I is an ideal, we must have that qx is in I so that $r = y - qx$ is in I. But as such, the minimality of x precludes the possibility that $\upsilon(r) < \upsilon(x)$, hence we must have that $r = 0_R$, from which we conclude that $y = qx$ is in xR and $I \subseteq xR$, as desired. □

Q2, January 2019. Consider the ring $R = \mathbb{C}[t, t^{-1}]$ of Laurent polynomials over $\mathbb{C}$.

(b.) Prove that every ideal in R is principal.

(c.) Give with proof an example of a nonzero prime ideal in R.

Contrapositively, Proposition 6 states that if R is an integral domain in which there exists an ideal that *is not* principal, then R is not a Euclidean domain. We put this to use immediately.

Example 4. Consider the ideal $I = (2, x)$ of the polynomial ring $\mathbb{Z}[x]$. On the contrary, we will assume that I is principal, i.e., we will assume that $I = f(x)\mathbb{Z}[x]$ for some polynomial $f(x)$ in $\mathbb{Z}[x]$. Considering that $2 = 2 \cdot 1 + x \cdot 0$ is in I, we must have that 2 is in $f(x)\mathbb{Z}[x]$, hence there exists a polynomial $g(x)$ such that $2 = f(x)g(x)$. One can easily verify that in $\mathbb{Z}[x]$, we have that $\deg f(x)g(x) = \deg f(x) + \deg g(x)$, from which it follows that $f(x)$ and $g(x)$ are both constant (i.e., integers). Considering the elements 2, $f(x)$, and $g(x)$ as integers, the primality of the integer 2 implies that either $f(x) = \pm 2$ or $f(x) = \pm 1$. But in any case, we have a contradiction: if $f(x) = \pm 2$, then x is not in $f(x)\mathbb{Z}[x]$; if $f(x) = \pm 1$, then $I = f(x)\mathbb{Z}[x] = \mathbb{Z}[x]$ despite the fact that 1 is not in I. By the contrapositive of Proposition 6, it follows that $\mathbb{Z}[x]$ is not a Euclidean domain.

Our previous example illustrates that the contrapositive of Proposition 6 affords a tool to decipher when an integral domain is not a Euclidean domain. One can show that for any prime integer p, the ideal (p, x) of $\mathbb{Z}[x]$ is not principal; however, we shall soon see that there exist non-Euclidean integral domains in which all ideals are principal, hence the task of finding non-principal ideals of an arbitrary integral domain becomes more complicated (and sometimes impossible) in general.

Existence of Greatest Common Divisors

Let R be a commutative ring. Continuing our generalization of the familiar properties of $\mathbb{Z}$, we make the following definitions. Given any elements r and $s \neq 0_R$ of R, we say that

(a.) s is a **divisor** of r (or equivalently, r is a **multiple** of s) whenever there exists an element t of R such that $r = st$, in which case we write $s \,|\, r$; and we say that

(b.) d is a **greatest common divisor** of r and s whenever

(i.) $d \,|\, r$ and $d \,|\, s$ and

(ii.) if $d' \,|\, r$ and $d' \,|\, s$, then $d' \,|\, d$.

Observe that in this sense, d is a divisor of r and s that is maximal with respect to divisibility.

Proposition 7. Given any elements r and $s \neq 0_R$ of a commutative ring R, we have that $s \,|\, r$ if and only if r is an element of the principal ideal $(s) = sR$ if and only if $(r) \subseteq (s)$.

Proof. We leave the (straightforward) details as an exercise to the reader. □

By Proposition 7, it follows that d is a greatest common divisor of r and s if and only if

(i.) $(r) \subseteq (d)$ and $(s) \subseteq (d)$ and

(ii.) if $(r) \subseteq (d')$ and $(s) \subseteq (d')$, then $(d) \subseteq (d')$

if and only if

(1.) $(r, s) \subseteq (d)$ and

(2.) if $(r, s) \subseteq (d')$, then $(d) \subseteq (d')$.

Proposition 8. Given any elements r and s of a commutative ring R, we have that d is a greatest common divisor of r and s if and only if d generates the unique minimal (with respect to inclusion) principal ideal that contains the ideal (r, s). Consequently, any subset S of at least two elements of a Euclidean domain gives rise to a greatest common divisor of the elements of S.

Recall that the greatest common divisor of two integers a and b is unique up to sign. Conventionally, we take $\gcd(a, b)$ to be positive. We may generalize this property to arbitrary integral domains.

Proposition 9. Let R be an integral domain. If x and y generate the same principal ideal in R, then there exists a unit u of R such that $y = xu$. (We say in this case that x and y are **associates**.) Consequently, the greatest common divisor of two elements is unique (up to a factor of a unit).

Proof. Given that $x = 0_R$, it follows that $y = 0_R$ by hypothesis that $xR = yR$ (from which we must have that $y = y \cdot 1_R = xr = 0_R r = 0_R$ for some element r of R). Consequently, we may assume that neither x nor y is zero. By hypothesis that $xR = yR$, it follows that there exists an element u of R such that $xu = y \cdot 1_R = y$. We claim that u is a unit. By the same rationale, there exists an element v of R such that $x = x \cdot 1_R = yv$, from which it follows that $y = xu = (yv)u = yuv$. Using the cancellative property of R, we have that $uv = 1_R$ (equivalently, we have that $y(1_R - uv) = y - yuv = 0_R$ and y is nonzero by hypothesis), as desired.

Given that d and d' are greatest common divisors of some elements of R, it follows that $(d) \subseteq (d')$ and $(d') \subseteq (d)$ so that $dR = (d) = (d') = d'R$ and $d' = du$ for some unit u of R. □

Last, we obtain the so-called Bézout's Lemma for Euclidean domains.

Theorem 1. (Bézout's Lemma) Given any two nonzero elements r and s of a Euclidean domain, let d denote the last nonzero remainder obtained from the Euclidean Algorithm with r and s.

(i.) d is a greatest common divisor of a and b and

(ii.) $(d) = (r, s)$, hence there exist elements x and y of R such that $d = rx + sy$.

Corollary 1. Given any elements r, s, and t of a Euclidean domain R, if r divides st, then $\dfrac{r}{\gcd(r, s)}$ divides t, where $\gcd(r, s)$ denotes the greatest common divisor of r and s. Consequently, if r divides st and r and s are **relatively prime** (i.e., we have that $\gcd(r, s)$ is a unit in R), then r divides t.

Proof. By Bézout's Lemma, we obtain a greatest common divisor d of r and s. Further, there exist elements x and y of R such that $\gcd(r, s) = rx + sy$. from which it follows that

$$1_R = \frac{r}{\gcd(r, s)}x + \frac{s}{\gcd(r, s)}y.$$

By multiplying both sides of this identity by t, we find that

$$t = \frac{r}{\gcd(r, s)}xt + \frac{st}{\gcd(r, s)}y.$$

Considering that $\dfrac{r}{\gcd(r, s)}$ divides each of the terms on the right-hand side (by hypothesis that r divides st), we conclude that $\dfrac{r}{\gcd(r, s)}$ divides t, as desired. Given that $\gcd(r, s)$ is a unit, it follows that $\dfrac{r}{\gcd(r, s)} = r \gcd(r, s)^{-1}$ is in (r) so that $(r) = \left(\dfrac{r}{\gcd(r, s)}\right) \supseteq (t)$ implies that r divides t. □

Before we move on, we remark that properties analogous to those outlined in Propositions 7 and 8 hold for a least common multiple of two elements of a commutative ring. Given any nonzero elements of a commutative ring R, we say that ℓ is a **least common multiple** of r and s whenever

(i.) $r \mid \ell$ and $s \mid \ell$ and

(ii.) if $r \mid \ell'$ and $s \mid \ell'$, then $\ell \mid \ell'$.

Observe that in this sense, ℓ is a multiple of r and s that is minimal with respect to divisibility.

Proposition 10. Given any elements r and s of a commutative ring R, we have that ℓ is a least common multiple of r and s if and only if ℓ generates the unique maximal (with respect to inclusion) principal ideal that is contained in $(r) \cap (s)$. Consequently, any subset S of at least two elements of a Euclidean domain gives rise to a least common multiple of the elements of S.

Proposition 11. Given any two elements r and s of a Euclidean domain R, the least common multiple of r and s is unique (up to a factor of a unit). Further, we have that

$$rs = \gcd(r, s) \operatorname{lcm}(r, s),$$

where $\gcd(r, s)$ and $\operatorname{lcm}(r, s)$ are the respective greatest common divisor and least common multiple.

Principal Ideal Domains

Quite naturally, we say that an integral domain in which every ideal is principal is a **principal ideal domain (PID)**. We have already encountered examples of PIDs: by Proposition 6, every ideal of a Euclidean domain is principal, hence any Euclidean domain is a principal ideal domain.

Remark 1. There exist principal ideal domains that are not Euclidean domains. Unfortunately, examples of such are rather nontrivial; however, a construction of one can be found here.

Remark 2. By definition, every ideal of a PID R is principal, hence for any elements r and s of R, if d generates the principal ideal that contains both r and s, then we have that

(i.) d is unique (up to a factor of a unit);

(ii.) d is a greatest common divisor of r and s; and

(iii.) there exist elements x and y of R such that $d = rx + sy$.

Consequently, the greatest common divisor of two elements of a PID is well-defined; it satisfies Bézout's Lemma; and it is unique (up to a factor of a unit). Likewise, one can prove that the least common multiple of two elements of a PID is well-defined and unique (up to a factor of a unit).

Originally discovered by commutative algebraist Irving Kaplansky, our next proposition illustrates that certain properties of the prime ideals of an integral domain R determine the structure of R.

Proposition 12. If every prime ideal of an integral domain R is principal, then R is a PID.

Proof. We note that this is exactly Corollary 8 from the notes "Rings, Ideals, and Homomorphisms," hence we leave the proof as an exercise to the reader (or you may use the previous notes). (Recall that $\mathfrak{F} = \{I \subseteq R \,|\, I \text{ is an ideal and } I \text{ is principal}\}$ is Oka, hence an ideal that is maximal (with respect to inclusion) with respect to the property that it is not contained in $\mathfrak{F}$ is prime. Use this to prove that if there is a non-principal ideal of R, then there is a prime non-principal ideal of R.) □

One of the most remarkable and highly useful facts about principal ideal domains is the following.

Proposition 13. Every nonzero prime ideal of a PID is maximal.

Proof. Consider a nonzero prime ideal P of a PID R. By hypothesis, the ideal P is principal, hence we have that $P = pR$ for some element p of P. Let us assume that there exists an ideal I that satisfies $P \subseteq I \subseteq R$. By hypothesis, the ideal I is principal, hence we may assume that $I = xR$ for some element x of I. We claim that $I = P$ or $I = R$, hence P is maximal. Considering that $pR = P \subseteq I = xR$, it follows that $p = p \cdot 1_R = xy$ for some element y of R. Consequently, we have that xy is in P. By hypothesis that P is prime, it follows that x is in P or y is in P. Given that x is in P, it follows that xr is in P for all elements r of R (because P is an ideal) so that $I = xR \subseteq P$ and $I = P$. On the other hand, if y is in P, then $y = pr$ for some element r of R so that $p = xy = x(pr) = p(xr)$ implies that $xr = 1_R$. Considering that $1_R = xr \in I$, we have $I = R$. □

Corollary 2. Let R be a commutative ring. Given that the polynomial ring $R[x]$ is a PID (e.g., if $R[x]$ is a Euclidean domain), we must have that R is a field.

Proof. Considering that R is a subring of $R[x]$, it follows that R is a domain. Consider the surjective ring homomorphism $\varphi : R[x] \to R$ defined by $\varphi(p(x)) = p(0_R)$. By the First Isomorphism Theorem, we have that $R \cong R[x]/\ker\varphi$, hence $\ker\varphi$ is a (nonzero) prime ideal of $R[x]$. Consequently, by Proposition 13, $\ker\varphi$ is a maximal ideal of $R[x]$ so that $R \cong R[x]/\ker\varphi$ is a field, as desired. □

By the contrapositive of Corollary 2, if R is not a field, then the polynomial ring $R[x]$ is not a PID (and therefore, it is not a Euclidean domain). Consequently, the integral domain $\mathbb{Z}[x]$ is not a PID. Even though we had already seen this in Example 4, it is important to note that our original argument required us to find an ideal that was not principal; however, Corollary 2 is general.

Proposition 14. Given a PID R and a prime ideal P of R, we have that R/P is a PID.

Proof. If P is the zero ideal, then by the First Isomorphism Theorem (applied to the identity homomorphism), we have that $R/P \cong R$ is a PID, as desired. Otherwise, if P is nonzero, then P is maximal so that R/P is a field and hence a Euclidean domain and so a PID (by Proposition 6). □

Later, we shall endeavor to understand the structure of polynomial rings over fields, but for now, let us focus our attention on understanding the structure of the integral domain $\mathbb{Z}[x]$.

Unique Factorization Domains

Consider any positive integer n. By the Fundamental Theorem of Arithmetic, there exist prime integers $p_1, \ldots, p_k$ and non-negative integers $e_1, \ldots, e_k$ such that $n = p_1^{e_1} \cdots p_k^{e_k}$. Further, the primes p_i such that the integer e_i is positive are unique (up to relabelling of the subscripts). Our aim in this section is to generalize the Fundamental Theorem of Arithmetic to arbitrary integral domains. Consider a commutative ring R. We say that an element p of R is **prime** whenever the principal ideal pR is a prime ideal. Equivalently, we have that p is prime if and only if p is not a unit and

$$p \,|\, rs \text{ implies that either } p \,|\, r \text{ or } p \,|\, s.$$

Certainly, this should look familiar: it is the same as the definition of prime integers. We say that a nonzero non-unit element r of R is **irreducible** whenever r has the property that

$$r = st \text{ implies that either } s \text{ or } t \text{ is a unit.}$$

Proposition 15. Prime factorizations of nonzero elements of an integral domain are unique (up to multiplication of the prime factors by a unit and rearrangement of the prime factors).

Proof. Consider a nonzero element x of an integral domain R that can be factored into a product of (not necessarily distinct) primes. Given that $x = p_1 \cdots p_n$ and $x = q_1 \cdots q_m$ are two prime factorizations of x, we have that $p_1 \,|\, q_i$ for some integer $1 \leq i \leq n$. Relabelling the primes $q_1, \ldots, q_m$, if necessary, we may assume that $p_1 \,|\, q_1$. Consequently, there exists an element r_1 of R such that $q_1 = r_1 p_1$. By hypothesis that q_1 is prime, we have that $q_1 \,|\, p_1$ or $q_1 \,|\, r_1$. On the contrary, if it were the case that $q_1 \,|\, r_1$, then we would have that $r_1 = s_1 q_1$ for some element s_1 of R so that $q_1 = r_1 p_1 = (s_1 q_1) p_1 = q_1 (s_1 p_1)$. By hypothesis that R is an integral domain, we would have that $s_1 p_1 = 1_R$ so that p_1 is a unit — a contradiction. We conclude therefore that $q_1 \,|\, p_1$ so that $p_1 = t_1 q_1 = t_1 (r_1 p_1) = p_1 (r_1 t_1)$ for some element t_1 of R. By hypothesis that R is an integral domain, we have that $r_1 t_1 = 1_R$ so that r_1 is a unit. Ultimately, we find that $p_1 p_2 \cdots p_n = r_1 p_1 q_2 \cdots q_m$. Cancelling a factor of p_1 from each side, we obtain $p_2 \cdots p_n = r_1 q_2 \cdots q_m$. Continuing in this manner, it cannot be the case that either $n > m$ or $n < m$ (because this would give a product of primes equal to a unit — a contradiction), hence we must have that $m = n$. Further, after relabelling the prime factors q_i, if necessary, there exist units r_i of R such that $q_i = r_i p_i$ for each integer $1 \leq i \leq n$. □

Combined with the previous observation, the following proposition establishes that a prime factorization in an integral domain leads to a factorization by irreducible elements.

Proposition 16. Every prime element of an integral domain is irreducible.

Proof. Consider a prime element p of an integral domain R. We will assume that $p = rs$ for some elements r and s of R. We claim that either r or s is a unit. By hypothesis that $p = rs$, we must have that $p \,|\, r$ or $p \,|\, s$, as p is prime. Given that $p \,|\, r$, it follows that $r = pt$ for some element t of R so that $p = rs = (pt)s = p(st)$. Consequently, we have that $st = 1_R$ so that s is a unit, as desired. □

We say that an integral domain R is a **unique factorization domain** (UFD) if every nonzero non-unit element of R can be written as a product of (not necessarily distinct) irreducibles in a unique (up to multiplication by a unit and rearrangement of factors) manner. Put another way, an integral domain R is a UFD if and only if for every nonzero non-unit element r of R, there exist (not necessarily distinct) irreducible elements $p_1, \ldots, p_n$ such that

(i.) $r = p_1 \cdots p_n$ and

(ii.) if $r = q_1 \cdots q_m$ for some (not necessarily distinct) irreducibles $q_1, \ldots, q_m$, then $m = n$ and (relabelling the q_i, if necessary) $q_i = u_i p_i$ for some units $u_i \in R$ for each integer $1 \leq i \leq n$.

Bourbaki refer to a unique factorization domain as a **factorial** ring.

Remark 3. By the Fundamental Theorem of Arithmetic, the integers form a UFD. Conversely, the Fundamental Theorem of Arithmetic follows from the following more general fact.

Proposition 17. Every PID is a UFD. Consequently, every Euclidean domain is a UFD.

Q5, August 2014. Consider a PID R. Given $f, g \in R$, prove that $f^{1000} g^{1014} \in (f^{2014}, g^{2014})$.

Unfortunately, we are not quite prepared to give a proof of Proposition 17 yet. Before we do, we must understand more of the properties of UFDs. We begin with the following observations.

Proposition 18. Given any nonzero non-unit elements r and s of a UFD R, the elements $\gcd(r,s)$ and $\operatorname{lcm}(r,s)$ exist and are unique (up to multiplication by a unit).

Proof. By hypothesis that R is a UFD, we have that $r = up_1^{e_1} \cdots p_n^{e_n}$ and $s = vp_1^{f_1} \cdots p_n^{f_n}$ for some distinct irreducibles $p_1, \ldots, p_n$, units u and v of R, and integers $e_i, f_i \geq 0$. We leave it to the reader to establish that $\gcd(r,s) = p_1^{\min\{e_1,f_1\}} \cdots p_n^{\min\{e_n,f_n\}}$ and $\operatorname{lcm}(r,s) = p_1^{\max\{e_1,f_1\}} \cdots p_n^{\max\{e_n,f_n\}}$. □

Remark 4. Proposition 18 guarantees that in a UFD, for any subset S of (at least) two elements, a greatest common divisor and least common multiple exist; however, it is not true that Bézout's Lemma holds for an arbitrary UFD. We shall soon see that $\mathbb{Z}[x,y]$ is a UFD with $\gcd(x,y) = 1$; however, there do not exist polynomials $f(x,y), g(x,y) \in \mathbb{Z}[x,y]$ such that $xf(x,y) + yg(x,y) = 1$ because $0 = \deg 1 = \deg(xf(x,y) + yg(x,y)) = \max\{\deg x + \deg f, \deg y + \deg g\} \geq 1$ is impossible.

Proposition 19. Every irreducible element of a UFD is prime. Consequently, by Proposition 16, the irreducible elements of a UFD are precisely the prime elements of a UFD.

Proof. Consider an irreducible element p of a UFD R. Given that $p \,|\, rs$ for some nonzero elements r and s of R, we claim that either $p \,|\, r$ or $p \,|\, s$. By hypothesis that $p \,|\, rs$, we have that $rs = pt$ for some element t in R. Certainly, if either r or s were a unit, then the claim holds. Consequently, we may assume that r and s are nonzero non-units. Considering that R is a UFD, each of the elements r, s, and t has a factorization as a product of irreducibles. Explicitly, we have that $r = i_1 \cdots i_\ell$, $s = j_1 \cdots j_m$, and $t = k_1 \cdots k_n$ for some (not necessarily distinct) irreducible elements $i_1, \ldots, i_\ell, j_1, \ldots, j_m, k_1, \ldots, k_n$ of R. We have therefore that

$$i_1 \cdots i_\ell j_1 \cdots j_m = rs = pt = pk_1 \cdots k_n.$$

By hypothesis that p is an irreducible element of the UFD R, we must have that p is an associate (or unit multiple) of some element $i_1, \ldots, i_\ell, j_1, \ldots, j_m$ so that $p \,|\, r$ or $p \,|\, s$, as desired. □

Recall from the previous notes on "Rings, Ideals, and Homomorphisms" that a commutative ring R is Noetherian whenever R satisfies the **ascending chain condition (ACC) on ideals**, i.e., for every ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$ of R, there exists an integer $N \geq 1$ sufficiently large so that for all pairs of distinct integers $m, n \geq N$, we have that $I_m = I_n$. We say in this case that the ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$ **stabilizes** (or **terminates** or **becomes stationary**).

Proposition 20. Let R be a nonzero integral domain. The following are equivalent.

(i.) R is a UFD.

(ii.) Every nonzero prime ideal of R contains a nonzero principal prime ideal of R.

(iii.) Every irreducible element of R is prime, and R satisfies the ACC for principal ideals.

Proof. We will establish that (i.) and (ii.) are equivalent; then, we will demonstrate that (i.) and (iii.) are equivalent. We will conclude therefore that (ii.) $\iff$ (i.) $\iff$ (iii.), as desired.

(i.) $\implies$ (ii.): Given that R is a UFD, consider a nonzero prime ideal P of R. (One exists because there is at least one maximal (and hence prime) ideal of R that is nonzero by hypothesis that R is nonzero.) Considering that P is nonzero, there exists a nonzero non-unit element p in P. By assumption that R is a UFD, we may write $p = q_1 \cdots q_n$ for some (not necessarily distinct) irreducibles $q_1, \ldots, q_n$. Considering that $q_1 \cdots q_n$ is in P, we must have that some q_i is in P by the primality of P. By Proposition 19, the irreducible q_i is a prime element of R so that $q_i R$ is a nonzero principal prime ideal of R. Considering that $q_i r$ is in P for every element r of R, we conclude that $q_i R \subseteq P$ so that P contains the nonzero principal prime ideal $q_i R$.

(ii.) $\implies$ (i.): We will assume that each nonzero prime ideal of R contains a nonzero principal prime ideal. Consider the multiplicatively closed* set $S = \{s \in R \mid s = p_1 \cdots p_n \text{ for some primes } p_i\}$. Given a nonzero non-unit x in R, we will assume to the contrary that $xR \cap S = \emptyset$. Considering that the collection $\mathfrak{F} = \{I \subseteq R \mid I \text{ is an ideal that contains } xR \text{ and } I \cap S \neq \emptyset\}$ comprises an Oka family**, there exists a nonzero prime ideal P of R containing xR that is maximal with respect to the property that $P \cap S = \emptyset$. By hypothesis, there exists a nonzero principal prime ideal pR in P. But then, we would have that $P \cap S \neq \emptyset$ — a contradiction. We must have therefore that $xR \cap S \neq \emptyset$ so that there exists an element $s \in xR \cap S$. By definition, we have that $s = xt$ for some element $t \in R$. Given that s is prime, then as every prime is irreducible, t must be a unit by hypothesis that x is not a unit, hence we have that $x = t^{-1}s$ is a factorization of x into a unit multiple of an irreducible. By Proposition 15, this is unique, hence R is a UFD. Continuing by induction, if $p_1 \cdots p_n = s = xt$, then by the primality of the p_i, either some $p_i \mid t$ or all $p_i \mid x$. If the former is true, then we may cancel p_i to obtain $xt' = p_1 \cdots p_{i-1} p_{i+1} \cdots p_n$, and we are done by induction. If the latter is true, then $x = p_1 \cdots p_n q$ so that $p_1 \cdots p_n = xt = tp_1 \cdots p_n q$ for some element $q \in R$ so that $tq = 1_R$, and q is a unit. Either way, the implication is proved by Proposition 15.

(i.) $\implies$ (iii.): Given that R is a UFD, it follows that every irreducible element of R is prime by Proposition 19. Consider an ascending chain of principal ideals $a_1 R \subseteq a_2 R \subseteq \cdots$ of R. By Proposition 7, we have that $a_i R \subseteq a_{i+1} R$ if and only if $a_{i+1} \mid a_i$ so that $a_i = a_{i+1} r_i$ for some element r_i of R and $a_i R = a_{i+1} R$ if and only if r_i is a unit. Consequently, for any strict containment of ideals $a_i R \subsetneq a_{i+1} R$, expanding both sides of the identity $a_i = a_{i+1} r_i$ in terms of the unique prime factorizations of a_i, a_{i+1}, and r_i illustrates that a_{i+1} must have strictly fewer irreducible factors than a_i. We conclude that $a_1 R \subseteq a_2 R \subseteq \cdots$ stabilizes, hence R has the ACC on principal ideals.

(iii.) $\implies$ (i.): Let R be an integral domain in which every irreducible element is prime, and R satisfies the ACC on principal ideals. We claim that every nonzero non-unit element of R has a unique factorization into a product of (not necessarily distinct) irreducible elements of R. On the contrary, we will assume that there exists a nonzero non-unit element x with no irreducible factorization in R. By hypothesis that x is not a unit, it follows that x cannot be irreducible (because if it were, it would be its own irreducible factorization), hence there exist nonzero non-units r_1 and s_1 so that $x = r_1 s_1$. Given that r_1 and s_1 both have irreducible factorizations, we would obtain an irreducible factorization of x. Consequently, one of r_1 or s_1 does not have an irreducible factorization — say $x_2 = r_1$ does not. By the same rationale as before, x_2 cannot be irreducible, so we have that $x_2 = r_2 s_2$ for some nonzero non-units r_2 and s_2. Continuing in this manner, we obtain a sequence $x, x_2, x_3, \ldots$ such that $x_{i+1} \mid x_i$. By Proposition 7, this induces an ascending chain

of principal ideals $xR \subseteq x_2R \subseteq x_3R \subseteq \cdots$ of R that does not stabilize — a contradiction. We conclude that every nonzero non-unit element of R has a factorization into (not necessarily distinct) irreducible elements of R. By hypothesis that the irreducible elements of R are prime, we conclude that every nonzero non-unit element of R has a factorization into a product of prime elements of R. By Proposition 15, such a factorization is unique in the sense of (ii.) in the definition of UFD. □

*We say that a subset S of a commutative ring R is **multiplicatively closed** whenever for any two elements r and s of S, we have that rs is in S. For instance, prove that if P is a prime ideal of a commutative ring R, then $R \setminus P$ (the set complement of P in R) is multiplicatively closed.

**One should show the more general statement that for any multiplicatively closed subset S of a commutative ring R, we have that $\mathfrak{F} = \{I \subseteq R \,|\, I \text{ is an ideal and } I \cap S \neq \emptyset\}$ is an Oka family.

Proof. (Proposition 17) Let R be a PID. Considering that every ideal of R is principal, for any nonzero prime ideal P of R, there exists a nonzero element p of P such that $P = pR$, and p must be a prime element of R. By the second criterion of Proposition 20, we conclude that R is a UFD. □

Observe that Proposition 17 gives another way to see that $\mathbb{Z}$ is a UFD. Even more, every Euclidean domain (and hence every field) is a UFD. Our next objective is to establish the following.

Proposition 21. We have that R is a UFD if and only if $R[x]$ is a UFD.

Like before with Proposition 17, we are not yet equipped with the tools to establish this fact. Let R be an integral domain in which any pair of elements (hence any collection of at least two elements) has a greatest common divisor (e.g., let R be a UFD). By Proposition 1, we have that $R[x]$ is an integral domain. Given a polynomial $f(x) = r_n x^n + \cdots + r_1 x + r_0$ in $R[x]$, we define the **content** of $f(x)$ to be the element $\text{content}(f) = \gcd(r_0, r_1, \ldots, r_n)$ of R. One might say that a polynomial $f(x)$ is **primitive** whenever $\text{content}(f)$ is a unit; however, this terminology will eventually become ambiguous, hence we will put it in quotation marks. Our next observation is quite natural.

Proposition 22. Let R be an integral domain in which any pair of elements has a greatest common divisor (e.g., let R be a UFD). Every polynomial $f(x) = r_n x^n + \cdots + r_1 x + r_0$ in $R[x]$ can be written as $f(x) = \text{content}(f)g(x)$ for some "primitive" polynomial $g(x)$ in $R[x]$.

Proof. By definition, $\text{content}(f) = \gcd(r_0, r_1, \ldots, r_n)$ divides each of the coefficients of $f(x)$, hence

$$g(x) = \frac{f(x)}{\text{content}(f)} = \frac{r_n}{\text{content}(f)} x^n + \cdots + \frac{r_1}{\text{content}(f)} x + \frac{r_0}{\text{content}(f)}$$

is a polynomial in $R[x]$ with

$$\text{content}(g) = \gcd\left(\frac{r_0}{\text{content}(f)}, \frac{r_1}{\text{content}(f)}, \ldots, \frac{r_n}{\text{content}(f)}\right).$$

By Bézout's Lemma, there exist elements $d_0, d_1, \ldots, d_n$ of R such that

$$r_0 d_0 + r_1 d_1 + \cdots + r_n d_n = \gcd(r_0, r_1, \ldots, r_n) = \text{content}(f),$$

hence we have that

$$\frac{r_0}{\text{content}(f)}d_0 + \frac{r_1}{\text{content}(f)}d_1 + \cdots + \frac{r_n}{\text{content}(f)}d_n = 1_R.$$

We conclude therefore that

$$R = \left(\frac{r_0}{\text{content}(f)}, \frac{r_1}{\text{content}(f)}, \ldots, \frac{r_n}{\text{content}(f)}\right)$$

$$\subseteq \gcd\left(\frac{r_0}{\text{content}(f)}, \frac{r_1}{\text{content}(f)}, \ldots, \frac{r_n}{\text{content}(f)}\right)R = \text{content}(g)R$$

so that $1_R = \text{content}(g)r$ for some element r of R, i.e., $\text{content}(g)$ is a unit of R. □

Our next proposition gives a sufficient criterion for a "primitive" polynomial to be irreducible.

Proposition 23. Let R be an integral domain in which any pair of elements has a greatest common divisor (e.g., let R be a UFD). Given a polynomial $f(x)$ of $R[x]$ that is irreducible, $f(x)$ does not factor as a product of non-constant polynomials in $R[x]$. Conversely, if $f(x)$ is "primitive" and $f(x)$ does not factor as a product of non-constant polynomials in $R[x]$, then $f(x)$ is irreducible in $R[x]$. Consequently, a "primitive" polynomial in $R[x]$ is irreducible if and only if it does not factor as a product of non-constant polynomials in $R[x]$.

Proof. Given an irreducible polynomial $f(x)$ of $R[x]$, let us assume that $f(x) = g(x)h(x)$ for some polynomials $g(x), h(x) \in R[x]$. By assumption that $f(x)$ is irreducible, we must have that either $g(x)$ or $h(x)$ is a unit. By Proposition 2, either $g(x)$ or $h(x)$ is a constant. Put another way, if $f(x)$ factors as a product of polynomials in $R[x]$, then one of those polynomials must be constant.

Conversely, let us assume that $\text{content}(f)$ is a unit and $f(x)$ does not factor as a product of non-constant polynomials in $R[x]$. Consequently, every factorization of $f(x)$ is of the form $f(x) = Cg(x)$ for some constant C of R. Considering that C divides $f(x)$ and C is in R, we must have that C divides all coefficients of $f(x)$ so that C divides $\text{content}(f)$. By hypothesis that $\text{content}(f)$ is a unit, we conclude that C is a unit, hence $f(x)$ is irreducible in $R[x]$ by definition. □

Of course, it remains to check that the irreducible elements of R are irreducible in $R[x]$.

Proposition 24. Let R be an integral domain. An element r of R is irreducible as an element of R if and only if the constant polynomial r is irreducible as an element of $R[x]$.

Proof. Given that r is an irreducible element of R, let us assume that $r = f(x)g(x)$ for some polynomials $f(x), g(x) \in R[x]$. By Proposition 1, we have that $R[x]$ is an integral domain so that $0 = \deg r = \deg f(x)g(x) = \deg f(x) + \deg g(x)$, hence $f(x)$ and $g(x)$ are both constant polynomials, and we may therefore view them as elements of R. By hypothesis that r is irreducible in R, it follows that either $f(x)$ or $g(x)$ is a unit of R. By Proposition 2, every unit of R is a unit of $R[x]$.

Conversely, we will assume that the constant polynomial r is irreducible as an element of $R[x]$. Given that $r = st$ for some elements $s, t \in R$, we have that $r = st$ for the constant polynomials $s, t \in R[x]$. By hypothesis that r is irreducible as an element of $R[x]$, we conclude that either s or t is a unit of $R[x]$. Once again, by Proposition 2, we conclude that either s or t is a unit of R. □

Corollary 3. Let R be a UFD. Every nonzero non-unit element of $R[x]$ is the product of irreducible elements of $R[x]$. Even more, an irreducible element of $R[x]$ is either

(a.) an irreducible element of R or

(b.) a polynomial of positive degree in $R[x]$ with unit content that does not factor as a product of non-constant polynomials in $R[x]$.

Proof. Let $f(x)$ be a nonzero non-unit element of $R[x]$. We proceed by induction on $\deg f(x)$. Given that $\deg f(x) = 0$, we have that $f(x)$ is an element of R. By hypothesis that R is a UFD, it follows that $f(x)$ is the product of irreducible elements of R. By Proposition 24, an irreducible factorization in R gives rise to an irreducible factorization in $R[x]$, hence we are done.

We will assume now that $\deg f(x) \geq 1$. By Proposition 22, we may write $f(x) = \text{content}(f)g(x)$ for some polynomial $g(x)$ in $R[x]$ such that $\text{content}(g)$ is a unit. Considering that $\text{content}(f)$ is an element of the UFD R, it follows that $\text{content}(f)$ can be factored as the product of irreducible elements of R and hence (by Proposition 24) irreducible elements of $R[x]$. On the other hand, Proposition 23 implies that either $g(x)$ is an irreducible element of $R[x]$ or $g(x)$ can be written as the product of (at least) two polynomials $h(x)$ and $j(x)$ of positive degree. Given that $g(x)$ is irreducible, we are done; otherwise, we have that $g(x) = h(x)j(x)$ for some polynomials in $R[x]$ of positive degree. Considering that $\deg h(x), \deg j(x) < \deg g(x)$, we are done by induction. □

Q3a, August 2018. Prove that the polynomial $f(x) = x^5 + x^2 + 1$ is irreducible in $\mathbb{Z}_2[x]$.

Corollary 3 synthesizes the content of Propositions 22, 23, and 24 and completely describes the irreducible elements of $R[x]$. Using these criteria and the familiar analogs of $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$, we will soon develop some essential divisibility properties of polynomial rings over integral domains.

Observe that the ring of integers $\mathbb{Z}$ can be extended to a field $\mathbb{Q}$ (the rational numbers) by declaring that all of the nonzero integers have multiplicative inverses. Even more, we can accomplish this in such a way that the addition and multiplication operations in $\mathbb{Z}$ give rise to well-defined addition and multiplication operations in $\mathbb{Q}$. Explicitly, we have that

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \text{ and } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

for any rational numbers $\frac{a}{b}$ and $\frac{c}{d}$. Generally, an integral domain R can be extended to a field $\text{Frac}\, R$ that is referred to as the **field of fractions** of R. Later, we will describe this process rigorously as the localization of R at the prime ideal $0_R R$, but for now, we need only see that

$$\text{Frac}\, R = \left\{ \frac{r}{s} \,\middle|\, r, s \in R \text{ and } s \neq 0_R \right\}$$

is a field under the operations of addition and multiplication defined by

$$\frac{r}{s} + \frac{t}{u} = \frac{ru + st}{su} \text{ and } \frac{r}{s} \cdot \frac{t}{u} = \frac{rt}{su}.$$

Proposition 25. Let R be an integral domain with field of fractions $\text{Frac}\, R$.

(1.) The additive identity of $\text{Frac}\, R$ is $\frac{0_R}{1_R}$, and the multiplicative identity of $\text{Frac}\, R$ is $\frac{1_R}{1_R}$.

(2.) The integral domain R can be identified with the subring $\left\{ \dfrac{r}{1_R} \,\middle|\, r \in R \right\}$ of $\operatorname{Frac} R$.

Proof. Property (1.) is a straightforward verification. Property (2.) can be established by applying the First Isomorphism Theorem to the map $\iota : R \to \operatorname{Frac} R$ defined by $\iota(r) = \dfrac{r}{1_R}$. □

By Proposition 25, for any integral domain R with field of fractions k, the polynomial ring $R[x]$ can be identified with a subring of the polynomial ring $k[x]$ via the map $\iota_x : R[x] \to k[x]$ defined by

$$\iota_x(r_n x^n + \cdots + r_1 x + r_0) = \frac{r_n}{1_R} x^n + \cdots + \frac{r_1}{1_R} x + \frac{r_0}{1_R}.$$

Proof. (Proposition 21) By Corollary 3, every nonzero non-unit element of $R[x]$ is the product of irreducible elements of $R[x]$. Further, the irreducible factors must be irreducible elements of R or "primitive" irreducible polynomials of $R[x]$ of positive degree. Consequently, it remains to be seen that such a factorization is unique (in the sense of (ii.) in the definition of a UFD). By Proposition 22, our proof is complete once we establish the unique factorization of "primitive" polynomials into irreducible "primitive" polynomials. Indeed, we will assume that $f(x)$ is a "primitive" polynomial in $R[x]$ with a factorization $f(x) = f_1(x) \cdots f_n(x)$ such that each polynomial $f_i(x)$ is an irreducible element of $R[x]$. Given any element r of R such that $r \mid f_i(x)$, we have that $r \mid f(x)$ so that $r \mid \operatorname{content}(f)$. By hypothesis that $f(x)$ is "primitive," it follows that $\operatorname{content}(f)$ is a unit so that r is a unit. Considering that $\operatorname{content}(f_i) \mid f_i(x)$ for each integer $1 \leq i \leq n$, it follows that $f_1(x), \ldots, f_n(x)$ are all irreducible "primitive" polynomials. Consequently, by Proposition 25, it follows that the polynomials $f_1(x), \ldots, f_n(x)$ are irreducible in $k[x]$, where $k = \operatorname{Frac} R$ is the field of fractions of R. Considering that $k[x]$ is a UFD, it follows that the factorization of $f(x) = f_1(x) \cdots f_n(x)$ in $k[x]$ is unique (in the sense of (ii.) in the definition of a UFD). Put another way, if we repeat this process for another factorization $f(x) = g_1(x) \cdots g_m(x)$ for some irreducible polynomials $g_j(x)$ in $R[x]$, we must have that $m = n$ and (relabelling the polynomials $g_i(x)$, if necessary) $g_i(x) = u_i f_i(x)$ in $k[x]$ for some unit u_i of $k[x]$ for each integer $1 \leq i \leq n$. By Proposition 2, the units of $k[x]$ are precisely the units of k, hence we have that $u_i = r_i / s_i$ for some nonzero elements $r_i, s_i \in R$. Consequently, we obtain the polynomial identities $s_i g_i(x) = r_i f_i(x)$ in $R[x]$. We have already established that the irreducible factors of a "primitive" polynomial are "primitive," hence we have that $\operatorname{content}(g_i)$ is a unit of R so that $s_i \operatorname{content}(g_i) = \operatorname{content}(s_i g_i) = \operatorname{content}(r_i f_i) = r_i \operatorname{content}(f_i)$ implies that $r_i = [\operatorname{content}(f_i)^{-1} \operatorname{content}(g_i)] s_i$. Consequently, we have that $u_i = r_i / s_i$ is a unit of R so that $f_i(x) = u_i g_i(x)$ for some unit $u_i \in R[x]$ for each integer $1 \leq i \leq n$.

Conversely, we will assume that $R[x]$ is a UFD. Given any nonzero non-unit element r of R, by viewing r as a constant polynomial in $R[x]$, it follows by hypothesis that $R[x]$ is a UFD that r has a unique (up to multiplication by a unit) factorization into irreducible elements of $R[x]$. By Proposition 24, we obtain a factorization of r into irreducible elements of R. Consequently, it suffices to check the uniqueness of this factorization. Consider any two factorizations $r = p_1 \cdots p_n$ and $r = q_1 \cdots q_m$ of r into irreducible elements of R. By viewing these as factorizations in $R[x]$, we conclude that $m = n$ and (relabelling the q_i, if necessary) $q_i = u_i p_i$ for some unit $u_i \in R[x]$ for each integer $1 \leq i \leq n$. By Proposition 2, the u_i are units of R, hence our proof is complete. □

We have therefore established that a commutative ring R is a UFD if and only if the univariate polynomial ring $R[x]$ is a UFD. Consequently, a commutative ring R is a UFD if and only if $R[x]$

is a UFD if and only if the univariate polynomial ring over $R[x]$ is a UFD, i.e., if and only if

$$R[x][y] = \{f_n(x)y^n + \cdots + f_1(x)y + f_0(x) \,|\, n \geq 0 \text{ is an integer and } f_0(x), f_1(x), \ldots, f_n(x) \in R[x]\}$$

is a UFD. Each polynomial $f_i(x)$ in $R[x]$ can be written as $f_i(x) = r_{d_i}x^{d_i} + \cdots + r_{1_i}x + r_{0_i}$ for some integer $d_i \geq 0$ and some coefficients $r_{0_i}, r_{1_i}, \ldots, r_{d_i} \in R$. Expanding each of the polynomials $f_i(x)$, we find that every element of $R[x][y]$ is a polynomial in the variables x and y. On the other hand, it is not difficult to see that for a rng R, the collection of bivariate polynomials over R given by

$$R[x, y] = \{r_n x^{a_n} y^{b_n} + \cdots + r_1 x^{a_1} y^{b_1} + r_0 \,|\, a_i, b_i, n \geq 0 \text{ are integers and } r_0, r_1, \ldots, r_n \in R\}$$

is a rng (with respect to the usual polynomial addition and multiplication) that inherits many of the properties of R. Using this notation, we have that $R[x][y] \subseteq R[x, y]$. Conversely, for any bivariate polynomial $f(x, y) = r_n x^{a_n} y^{b_n} + \cdots + r_1 x^{a_1} y^{b_1} + r_0$, if $d = \max\{b_1, \ldots, b_n\}$, then $f(x, y) = f_d(x)y^d + \cdots + f_1(x)y + f_0(x)$ for some polynomials $f_0(x), f_1(x), \ldots, f_d(x) \in R[x]$. For example, the polynomial $f(x, y) = 3x^3y^3 - 5x^3y^2 + x^3y - x^2y^3 - 7x^2 + y + 2y^3$ in $\mathbb{Z}[x, y]$ can be written as the polynomial $(3x^3 - x^2 + 2)y^3 + (-5x^3)y^2 + (x^3 + 1)y - 7x^2$ in $\mathbb{Z}[x][y]$. Certainly, if we view the polynomial ring $R[y][x]$ similarly to $R[x][y]$, then we have established the following proposition.

Proposition 26. Given a rng R, we have that $R[x][y] = R[x, y] = R[y][x]$.

Corollary 4. Let R be a UFD. For any integer $n \geq 1$, the polynomial ring $R[x_1, \ldots, x_n]$ is a UFD. Further, the polynomial ring $R[x_1, x_2, \ldots]$ in countably many variables is a UFD.

Proof. By Proposition 21, if R is a UFD, then $R[x]$ is a UFD so that $R[x_1, x_2] = R[x_1][x_2]$ is a UFD. By induction, therefore, we have that $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$ is a UFD.

Observe that $R[x_1]$ can be identified with a subring of $R[x_1, x_2]$ by the First Isomorphism Theorem applied to the ring homomorphism $\varphi : R[x_1] \to R[x_1, x_2]$ defined by

$$\varphi(r_n x_1^n + \cdots + r_1 x_1 + r_0) = r_n x_1^n + \cdots + r_1 x_1 + r_0 + 0_R x_2.$$

Consequently, we have an ascending chain of polynomial rings $R[x_1] \subseteq R[x_1, x_2] \subseteq \cdots$ so that

$$R[x_1, x_2, \ldots] = \bigcup_{n=1}^{\infty} R[x_1, \ldots, x_n]$$

is a ring whose elements are polynomials in finitely many variables. Each of the rings $R[x_1, \ldots, x_n]$ is a UFD, hence a polynomial f in $R[x_1, x_2, \ldots]$ has a unique factorization in $R[x_1, \ldots, x_n]$, where n is the largest subscript of a variable appearing in f. Our proof is therefore complete. □

Q1, January 2018. Consider the ring $R = \mathbb{C}[x, y, z]$ and the prime ideal $I = (x, y)$.

(b.) Prove that for any collection of polynomials $\{f_1, \ldots, f_n\}$ such that $f_1 \cdots f_n$ is in $J = (x^2, y^2)$, there exists a subset of at most three polynomials whose product is in J.

(c.) Prove that for any collection of polynomials $\{f_1, \ldots, f_n\}$ such that the product $f_1 \cdots f_n$ is in $K = (x^2y^2, x^2z^2, y^2z^2)$, there exist at most nine polynomials whose product is in K.

Polynomial Rings over UFDs

By Proposition 21, the univariate polynomial ring $R[x]$ is a UFD if and only if the ring of coefficients R is a UFD. Further, by Proposition 17, a Euclidean domain is a UFD. We have seen in Example 1 that a field is a Euclidean domain. Consequently, for any integral domain R, we have that $k[x]$ is a UFD, where $k = \operatorname{Frac} R$ is the field of fractions of R. We have already seen in the proof of Proposition 21 the power of the technique of passing to the field of fractions of an integral domain R. Our next objective is to exploit this technique further to study the factorization of a polynomial of $f(x)$ over a UFD R in terms of its factorization in $k[x]$.

Proposition 27. Let R be a UFD with field of fractions k. Consider a "primitive" polynomial $g(x)$ in $R[x]$. Observe that $g(x)$ may be viewed as a polynomial in $k[x]$ in the manner described on page 13. If we have that $g(x) \mid f(x)$ as polynomials in $k[x]$, then $g(x) \mid f(x)$ as polynomials in $R[x]$.

Proof. We will assume that $g(x) \mid f(x)$ as polynomials in $k[x]$. By definition, there exists a polynomial $h(x)$ in $k[x]$ such that $f(x) = g(x)h(x)$. Explicitly, we may write

$$h(x) = \frac{n_i}{d_i}x^i + \cdots + \frac{n_1}{d_1}x + \frac{n_0}{d_0}$$

for some nonzero elements $d_0, d_1, \ldots, d_i$ of R. Consider the element $d = d_0 d_1 \cdots d_i$. By hypothesis that $d_0, d_1, \ldots, d_i$ are nonzero in R and R is an integral domain, it follows that d is a nonzero element of R such that $dh(x)$ is in $R[x]$ (under the identification above; in truth, the denominators of the coefficients of $h(x)$ are all 1_R). Consequently, we have that $df(x) = g(x)[dh(x)]$ so that $g(x) \mid df(x)$ in $R[x]$. We have therefore established that the set $C = \{c \in R : g(x) \mid cf(x) \text{ in } R[x]\}$ is nonempty. Consider an element m of C with the least number of irreducible factors. (Observe that this quantity is well-defined by the Well-Ordering Principle.) Given that m is a unit, we are done because we would have that $f(x) = g(x)[m^{-1}j(x)]$ for some polynomial $j(x)$ of $R[x]$. On the contrary, we will assume that m is not a unit. Consequently, there is some irreducible element r of R such that $r \mid m$. Considering that $mf(x) = g(x)j(x)$ for some polynomial $j(x)$ in $R[x]$ and $r \mid m$, we have that $r \mid g(x)j(x)$. By hypothesis that R is a UFD, an irreducible element of R is prime, hence we must have that $r \mid g(x)$ or $r \mid j(x)$. Given that $r \mid g(x)$, it follows that r divides content(g) so that r is a unit — a contradiction. Given that $r \mid j(x)$, then we have the polynomial identity

$$g(x)\frac{j(x)}{r} = \frac{g(x)j(x)}{r} = \frac{mf(x)}{r} = \frac{m}{r}f(x)$$

in $R[x]$ so that $g(x)$ divides $(m/r)f(x)$ in $R[x]$ — contradicting the definition of m. □

Put another way, Proposition 27 states that if a polynomial of $R[x]$ has a "primitive" factor when viewed as a polynomial in $k[x]$, then that "primitive" factor remains a factor when considered as a polynomial of $R[x]$. Our next proposition generalizes this to any factorization in $k[x]$.

Proposition 28. (Gauss's Lemma) Let R be a UFD with field of fractions k. Consider a polynomial $f(x)$ in $R[x]$. If there exist polynomials $G(x)$ and $H(x)$ in $k[x]$ such that $f(x) = G(x)H(x)$, then there exist polynomials $g(x)$ and $h(x)$ in $R[x]$ such that $f(x) = g(x)h(x)$.

Proof. We will assume that $f(x) = G(x)H(x)$ for some polynomials $G(x)$ and $H(x)$ in $k[x]$. By the proof of Proposition 27, we may "clear the denominators" of the coefficients of $G(x)$ to obtain a polynomial $g_{\text{red}}(x) = d_G G(x)$ of $R[x]$. By Proposition 22, we may factor the polynomial $g_{\text{red}}(x)$ of $R[x]$ as $g_{\text{red}}(x) = \text{content}(g)g(x)$ for some polynomial $g(x)$ in $R[x]$ with unit content. We have therefore established that $g(x) \mid f(x)$ in $k[x]$, as we have the polynomial identity

$$f(x) = G(x)H(x) = \frac{1_R}{d_G} g_{\text{red}}(x)H(x) = \frac{\text{content}(g)}{d_G} g(x)H(x) = g(x) \cdot \frac{\text{content}(g)}{d_G} H(x).$$

By Proposition 27, there exists a polynomial $h(x)$ in $R[x]$ such that $f(x) = g(x)h(x)$ in $R[x]$. □

Corollary 5. (Gauss's Little Lemma) Consider the polynomial ring $\mathbb{Z}[x]$ over the integers.

(i.) If $f(x)$ and $g(x)$ are polynomials in $\mathbb{Z}[x]$ such that $\text{content}(f) = \pm 1$ and $\text{content}(g) = \pm 1$, then $f(x)g(x)$ is a polynomial of $\mathbb{Z}[x]$ whose content is ± 1.

(ii.) Given a polynomial $f(x)$ of positive degree with $\text{content}(f) = \pm 1$, we have that $f(x)$ is irreducible in $\mathbb{Z}[x]$ if and only if $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Remark 5. Gauss's Little Lemma holds for an arbitrary UFD R by replacing every instance of $\mathbb{Z}$ with R, every instance of $\mathbb{Q}$ with $\text{Frac}\, R$, and every instance of ± 1 with "a unit of R."

Q2, August 2017. Let R be a UFD with field of fractions k. Given a nonzero polynomial $f(x)$ in $R[x]$, consider the ideals $I = f(x)R[x]$ and $J = (f(x)k[x]) \cap R[x]$ of $R[x]$. Prove that there exists a nonzero element c in R such that $I = cJ$ as ideals of R.

Q2a, January 2019. Prove that $\mathbb{C}[t, t^{-1}] \cong \mathbb{C}[x, y]/(xy - 1)$.

Q2, January 2010. Let $\varphi : \mathbb{C}[x, y] \to \mathbb{C}[t, t^{-1}]$ be the $\mathbb{C}$-algebra homomorphism defined by $\varphi(f(x, y)) = f(t, t^{-1})$. Find with proof a polynomial $g(x, y)$ such that $\ker(\varphi) = (g(x, y))$. Further, prove that there is an isomorphism of $\mathbb{C}$-algebras from $\mathbb{C}[x, y]/(x^2 + y^2 - 1)$ to $\mathbb{C}[t, t^{-1}]$.

Gauss's Little Lemma guarantees that a "primitive" irreducible polynomial over a UFD remains irreducible when considered as a polynomial over the field of fractions. Our next proposition illustrates a sufficient condition for a "primitive" polynomial over a UFD to be irreducible.

Proposition 29. (Eisenstein's Criterion) Let R be an integral domain in which any pair of elements has a greatest common divisor (e.g., let R be a UFD) with field of fractions k. Given a polynomial $f(x) = r_n x^n + \cdots + r_1 x + r_0$ of $R[x]$, if there exists a prime ideal P of R such that

(i.) $r_0, r_1, \ldots, r_{n-1} \in P$,

(ii.) $r_n \notin P$, and

(iii.) $r_0 \notin P^2$,

then $f(x)$ cannot be written as the product of two non-constant polynomials. Consequently, if $f(x)$ is "primitive," then $f(x)$ is irreducible over $R[x]$, hence $f(x)$ is irreducible over $k[x]$.

Proof. On the contrary, we will assume that $f(x) = g(x)h(x)$ for some non-constant polynomials $g(x)$ and $h(x)$ of $R[x]$. We may write $g(x) = a_i x^i + \cdots + a_1 x + a_0$ and $h(x) = b_j x^j + \cdots + b_1 x + b_0$ for some elements $a_0, a_1, \ldots, a_i, b_0, b_1, \ldots, b_j \in R$. Consequently, we have that $r_0 = a_0 b_0$, $r_1 = a_1 b_0 + a_0 b_1$, etc. By hypothesis that $r_0 \in P$ and $r_0 \notin P^2$, we must have that $a_0 \in P$ or $b_0 \in P$ but not both. We may assume that $a_0 \in P$. We have therefore that $0_R + P = r_1 + P = a_1 b_0 + a_0 b_1 + P = a_1 b_0 + P$. Considering that $a_0 \in P$, we must have that $b_0 \notin P$ so that $a_1 \in P$. Continuing in this manner, we find that $a_0, a_1, \ldots, a_i \in P$ so that $r_n = a_i b_j$ is in P — a contradiction. We conclude that either $g(x)$ or $h(x)$ is a constant polynomial in $R[x]$. By Proposition 23, if $f(x)$ is "primitive," then $f(x)$ is irreducible over $R[x]$. By Gauss's Little Lemma, we have that $f(x)$ is irreducible in $k[x]$. □

Q4a, August 2013. Prove that the polynomial $f(x) = x^3 - 2$ is irreducible in $\mathbb{Q}[x]$.

Q4a, January 2017. Prove that the polynomial $f(x) = x^3 - 9x + 3$ is irreducible in $\mathbb{Q}[x]$.

Consider any field k. By Example 3, we have that $k[x]$ is a Euclidean domain, hence $k[x]$ is a PID by Proposition 6, and ultimately, we have that $k[x]$ is a UFD by Proposition 17. By Proposition 19, therefore, every irreducible polynomial $p(x)$ in $k[x]$ is a prime element of $k[x]$ so that the principal prime ideal $(p(x)) = p(x)k[x]$ is maximal by Proposition 13. Consequently, every irreducible polynomial $p(x)$ with coefficients in a field k gives rise to a field $F = k[x]/(p(x))$. Later, we shall prove that F contains a subfield that is isomorphic to k and that F contains a root of $p(x)$; however, for now, we will restrict our attention to the structure of the ideals of the UFD $R[x]$.

Proposition 30. Let k be a field. Given an ideal I of $k[x]$, we have that I is maximal in $k[x]$ if and only if $I = p(x)k[x]$ for some irreducible polynomial $p(x)$ of $k[x]$.

Proof. By the previous paragraph, for any irreducible polynomial $p(x)$ of $k[x]$, the principal ideal $p(x)k[x]$ is maximal. Conversely, for any ideal I of $k[x]$, there exists a polynomial $f(x)$ in I such that $I = f(x)k[x]$ (because $k[x]$ is a PID). Given that $f(x)$ is not irreducible in $k[x]$, there exist non-constant polynomials $g(x)$ and $h(x)$ in $k[x]$ such that $f(x) = g(x)h(x)$. By Proposition 7, we have that $I = f(x)k[x] \subsetneq g(x)k[x] \subsetneq k[x]$ so that I is not a maximal ideal of $k[x]$. □

Consequently, a maximal ideal of a polynomial ring over a field must be the principal ideal generated an irreducible polynomial of $k[x]$. Our next propositions classify the maximal ideals of $\mathbb{Z}[x]$.

Lemma 1. Let R be a commutative ring with an ideal I. We have that

$$\frac{R}{I}[x] \cong \frac{R[x]}{I[x]},$$

where we define $I[x] = \{i_n x^n + \cdots + i_1 x + i_0 \,|\, n \geq 0 \text{ is an integer and } i_0, i_1, \ldots, i_n \in I\}$.

Proof. Consider the map $\varphi : R[x] \to (R/I)[x]$ defined by

$$\varphi(r_n x^n + \cdots + r_1 x + r_0) = (r_n + I)x^n + \cdots + (r_1 + I) + (r_0 + I).$$

We leave it to the reader to establish that φ is a surjective ring homomorphism with $\ker \varphi = I[x]$. □

Proposition 31. There are no principal maximal ideals of $\mathbb{Z}[x]$.

Proof. We will first show that no constant polynomial generates a maximal ideal. Given any integer n, consider the ideal $n\mathbb{Z}[x]$. Observe that $f(x)$ is in $n\mathbb{Z}[x]$ if and only if $f(x) = n(a_n x^n + \cdots + a_1 x + a_0)$ for some integer $n \geq 0$ and some integers $a_0, a_1, \ldots, a_n$ of R if and only if $f(x) = na_n x^n + \cdots + na_1 x + na_0$ if and only if $f(x)$ is in $(n\mathbb{Z})[x]$. Consequently, by Lemma 1, we have that

$$\frac{\mathbb{Z}[x]}{n\mathbb{Z}[x]} = \frac{\mathbb{Z}[x]}{(n\mathbb{Z})[x]} \cong \frac{\mathbb{Z}}{n\mathbb{Z}}[x] = \mathbb{Z}_n[x].$$

But this is not a field, hence $n\mathbb{Z}[x]$ is not a maximal ideal. On the other hand, consider a nonzero non-constant polynomial $f(x)$ of $\mathbb{Z}[x]$. On the contrary, we will assume that $I = f(x)\mathbb{Z}[x]$ is maximal so that $\mathbb{Z}[x]/I$ is a field. Consider a prime integer p that does not divide the leading coefficient of $f(x)$. Because $f(x)$ does not divide p, $p + f(x)\mathbb{Z}[x]$ is a nonzero element of the field $\mathbb{Z}[x]/I$ so that $p + f(x)\mathbb{Z}[x]$ is a unit. Consequently, there exists a polynomial $g(x)$ of $\mathbb{Z}[x]$ such that

$$g(x)p + f(x)\mathbb{Z}[x] = (g(x) + f(x)\mathbb{Z}[x])(p + f(x)\mathbb{Z}[x]) = 1 + f(x)\mathbb{Z}[x].$$

Unraveling this, by definition, there exists a polynomial $h(x)$ of $\mathbb{Z}[x]$ such that $g(x)p + f(x)h(x) = 1$ in $\mathbb{Z}[x]$. Using the ring homomorphism $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ of Lemma 1, we have therefore that

$$1 = \varphi(1) = \varphi(g(x)p + f(x)h(x)) = \varphi(g(x))\varphi(p) + \varphi(f(x))\varphi(h(x) = \varphi(f(x))\varphi(h(x))$$

in $\mathbb{Z}_p[x]$. By hypothesis that p does not divide the leading coefficient of $f(x)$, we must have that $\deg \varphi(f(x)) = \deg f(x)$. Considering that $\mathbb{Z}_p$ is a field, it follows that

$$0 = \deg 1 = \deg \varphi(f(x))\varphi(h(x)) = \deg \varphi(f(x)) + \deg \varphi(h(x)) \geq \deg \varphi(f(x)) = \deg f(x) > 0$$

— a contradiction. We conclude therefore that $f(x)\mathbb{Z}[x]$ is not a maximal ideal of $\mathbb{Z}[x]$. □

Proposition 32. Given an ideal I of $\mathbb{Z}[x]$, we have that I is maximal in $\mathbb{Z}[x]$ if and only if $I = (p, f(x))$ for some prime integer p and some polynomial $f(x)$ that is irreducible in $\mathbb{Z}_p[x]$.

Proof. Consider a maximal ideal M of $\mathbb{Z}[x]$. Observe that $\mathbb{Z}$ is a subring of $\mathbb{Z}[x]$, hence we may consider the ideal $M \cap \mathbb{Z}$, i.e., the contraction of M to the subring $\mathbb{Z}$. Considering that $0 \in M \cap \mathbb{Z}$, this ideal is nonempty. We claim moreover that $M \cap \mathbb{Z}$ contains nonzero elements. On the contrary, we will assume that $M \cap \mathbb{Z} = \{0\}$. Consequently, the only nonzero elements of M are non-constant polynomials of $\mathbb{Z}[x]$. We may identify $\mathbb{Z}[x]$ with a subring of $\mathbb{Q}[x]$ in the usual way (cf. page 13) and consider the ideal $M^e = \{m_1 f_1(x) + \cdots + m_n f_n(x) \,|\, n \geq 1,\ m_i \in M,\ \text{and } f_i(x) \in \mathbb{Q}[x]\}$ of $\mathbb{Q}[x]$. Considering that $\mathbb{Q}[x]$ is a PID, it follows that $M^e = q(x)\mathbb{Q}[x]$ for some nonzero non-constant polynomial $q(x)$ of $\mathbb{Q}[x]$. Clearly, content(q) is a unit in $\mathbb{Q}$, hence we may assume without loss of generality that content$(q) = 1$. (If not, then replace $q(x)$ with $r(x) = \frac{q(x)}{\text{content}(q)}$ to obtain $M^e = r(x)\mathbb{Q}[x]$.) By Gauss's Lemma, we have that $M = q(x)\mathbb{Z}[x]$ — contradicting Proposition 31.

On the other hand, observe that $M \cap \mathbb{Z}$ is the kernel of the ring homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}[x]/M$ defined by $\varphi(n) = n + M$. By the First Isomorphism Theorem, we may identify $\mathbb{Z}/(M \cap \mathbb{Z})$ with a subdomain of the field $\mathbb{Z}[x]/M$ so that $M \cap \mathbb{Z}$ is a prime ideal of the PID $\mathbb{Z}$. By the above paragraph, there exist nonzero elements in the ideal $M \cap \mathbb{Z}$, hence $M \cap \mathbb{Z}$ is a nonzero principal prime ideal of $\mathbb{Z}$. Put another way, there exists a prime integer p of $\mathbb{Z}$ such that $M \cap \mathbb{Z} = p\mathbb{Z}$.

Considering that p is an element of M, we have the ideal containment $p\mathbb{Z}[x] \subseteq M$ in $\mathbb{Z}[x]$, from which it follows that the map $\pi : \mathbb{Z}[x]/p\mathbb{Z}[x] \to \mathbb{Z}[x]/M$ defined by $\pi(f(x) + p\mathbb{Z}[x]) = f(x) + M$ is a well-defined surjective ring homomorphism. Observe that $f(x) + p\mathbb{Z}[x]$ is in $\ker \pi$ if and only if $f(x) + M = 0 + M$ so that $\ker \pi = M/p\mathbb{Z}[x]$. By the First Isomorphism Theorem and Lemma 1, we have that $M/p\mathbb{Z}[x]$ is a maximal ideal of the PID $\mathbb{Z}[x]/p\mathbb{Z}[x] \cong \mathbb{Z}_p[x]$. By Proposition 30, we find that $M/p\mathbb{Z}[x]$ is generated by an irreducible element $g(x) + p\mathbb{Z}[x]$ of $\mathbb{Z}[x]/p\mathbb{Z}[x]$. We claim that for any polynomial $f(x)$ of M such that $f(x) + p\mathbb{Z}[x] = g(x) + p\mathbb{Z}[x]$, we have that $M = (p, f(x))$.

Considering that $M/p\mathbb{Z}[x]$ is generated by $g(x) + p\mathbb{Z}[x]$, it follows that every element of $M/p\mathbb{Z}[x]$ is of the form $(g(x) + p\mathbb{Z}[x])(h(x) + p\mathbb{Z}[x]) = g(x)h(x) + p\mathbb{Z}[x]$. Unraveling this, we find that for every element m of M, there exists a polynomial $r(x)$ in $\mathbb{Z}[x]$ such that $m = g(x)h(x) + r(x)p$. Given that $f(x) + p\mathbb{Z}[x] = g(x) + p\mathbb{Z}[x]$, it follows that $g(x) = f(x) + s(x)p$ for some polynomial $s(x)$ of $\mathbb{Z}[x]$ so that $m = (f(x) + s(x)p)h(x) + r(x)p = f(x)h(x) + p(r(x) + s(x))$ is in $(p, f(x))$.

Conversely, we will establish that there exists a ring isomorphism

$$\frac{\mathbb{Z}[x]}{(p, f(x))} \cong \frac{\mathbb{Z}_p[x]}{f(x)\mathbb{Z}_p[x]},$$

from which it follows that $(p, f(x))$ is maximal whenever p is a prime integer and $f(x)$ is irreducible in $\mathbb{Z}_p[x]$. We will prove a more general fact that for any commutative ring R and any ideals I and J of R, we have that $(I + J)/J = I(R/J)$, where we define the ideal generated by I in R/J as

$$I(R/J) = \{(r_1 + J)(i_1 + J) + \cdots + (r_n + J)(i_n + J) \,|\, n \geq 0 \text{ is an integer, } i_k \in I, \text{ and } r_k \in R\}.$$

Once this is accomplished, it will follow by Lemma 1 and the Third Isomorphism Theorem that

$$\frac{\mathbb{Z}[x]}{(p, f(x))} = \frac{\mathbb{Z}[x]}{p\mathbb{Z}[x] + f(x)\mathbb{Z}[x]} \cong \frac{\mathbb{Z}[x]/p\mathbb{Z}[x]}{f(x)(\mathbb{Z}[x]/p\mathbb{Z}[x])} \cong \frac{(\mathbb{Z}/p\mathbb{Z})[x]}{f(x)(\mathbb{Z}/p\mathbb{Z})[x]} = \frac{\mathbb{Z}_p[x]}{f(x)\mathbb{Z}_p[x]}.$$

Of course, we have that $(r_1 + J)(i_1 + J) + \cdots + (r_n + J)(i_n + J) = (r_1 i_1 + \cdots + r_n i_n) + J$ is an element of $(I + J)/J$ because I is an ideal of R, hence it follows that $I(R/J) \subseteq (I + J)/J$. On the other hand, we have that $i + j + J = i + J = (1_R + J)(i + J)$ is an element of $I(R/J)$. □

Q2a, August 2010. Consider the polynomial ring $\mathbb{Z}[x]$. Prove that the ideals $M_1 = (3, x^2 + x + 2)$ and $M_2 = (2, x^2 + x + 1)$ of $\mathbb{Z}[x]$ are maximal in $\mathbb{Z}[x]$.

Q2a, August 2012. Prove that the ring $F = \mathbb{Z}_2[x]/(x^3 - x + 1)$ is a field.

Q2b, August 2018. Prove or disprove that $(2, x^2 + x + 1)$ is a maximal ideal in $\mathbb{Z}[x]$.

Q3, August 2015. Given the polynomial $f(x) = x^3 + 2$ in $\mathbb{Z}[x]$ and a root α of $f(x)$ in $\mathbb{C}$, consider the sets $K = \mathbb{Q}(\alpha)$ and $R = \{a + b\alpha + c\alpha^2 \,|\, a, b, c \in \mathbb{Z}\} \subset K$.

(b.) Prove that for every nonzero ideal I of $\mathbb{Z}$, we have that $IR \cap \mathbb{Z} = I$.

(c.) Prove that for every nonzero ideal J of R, we have that $J \cap \mathbb{Z} \neq \{0\}$.

(d.) Prove that every nonzero prime ideal in R is maximal.