Rings, Ideals, and Homomorphisms

Dylan C. Beck

Rings and the Hierarchy of Commutative Rings

Given an abelian group $(R, +)$ equipped with a map $\cdot : R \times R \to R$ that sends $(r, s) \mapsto r \cdot s$, we say that the triple $(R, +, \cdot)$ is a **ring** whenever the following properties hold for R.

(i.) The map $\cdot$ is associative, i.e., we have that $r \cdot (s \cdot t) = (r \cdot s) \cdot t$ for any r, s, and t in R.

(ii.) The map $\cdot$ is distributive, i.e., we have that $r \cdot (s + t) = r \cdot s + r \cdot t$ and $(r + s) \cdot t = r \cdot t + s \cdot t$ for any elements r, s, and t in R.

(iii.) There exists an element 1_R of R such that $1_R \cdot r = r = r \cdot 1_R$ for all elements r of R.

Corollary 1. For every element r of a ring, we have that $r0_R = 0_R$.

Proof. We leave the proof as an exercise for the reader. □

One can show that the element 1_R is unique; it is the **multiplicative identity** (or **unity**) of R.

Remark 1. Even though this situation is growing increasingly uncommon over time, it is possible to come across an author who defines a ring as an abelian group with a multiplication that satisfies properties (i.) and (ii.) *but not necessarily* property (iii.). We refer to such an algebraic structure as a **rng** because it has no "i"dentity; however, these authors refer to our rings as **unital rings**.

Remark 2. Given an element r of R such that there exists an element s of R with $rs = 1_R = sr$, we refer to r as a **unit**. One can show that the element s is unique; it is the **multiplicative inverse** of r, hence we may write $s = r^{-1}$. We have made no assumption that every nonzero element of R has a multiplicative inverse; in fact, a ring with this property is called a **skew field**.

Usually, we will omit the multiplicative notation $\cdot$ of R and simply use concatenation, e.g., $r \cdot s \stackrel{\text{def}}{=} rs$. Given a nonempty set $S \subseteq R$, we say that S is a **subring** of R whenever S is a ring with respect to the operation of R. Often, it is convenient to use the following proposition.

Proposition 1. (Subring Test) Given a ring R and a set $S \subseteq R$ containing 1_R such that for all elements r and s in S, we have that $r - s$ and rs are in S, it follows that S is a subring of R.

Q3a, August 2015. Given the polynomial $f(x) = x^3 + 2$ (viewed as an element of the polynomial ring $\mathbb{Z}[x]$) and a root α of $f(x)$ in $\mathbb{C}$, consider the set $K = \mathbb{Q}(\alpha)$ of rational functions in α with rational coefficients. Prove that the set $R = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Z}\}$ is a subring of K.

Our primary focus will involve **commutative** rings, i.e., rings for which the multiplication is commutative (so that $rs = sr$ for all r and s in R); however, there exist noncommutative rings.

Example 1. Given a positive integer n, consider the set $\mathbb{Z}^{n\times n}$ of $n \times n$ matrices with integer entries. Observe that $\mathbb{Z}^{n\times n}$ is a ring with respect to matrix addition and matrix multiplication: its identity is the identity matrix I_n whose (i, j)th entry is the Kronecker delta δ_{ij} for all integers $1 \leq i, j \leq n$. We note that $\mathbb{Z}^{n\times n}$ is noncommutative for any integer $n \geq 2$ because for any integers a, b, c and d such that $ac \neq bc$ and $ad \neq bd$, we have that $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & c \\ d & 0 \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 0 & c \\ d & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$. Considering these matrices as 2×2 submatrices of any matrix of size $n \geq 3$ gives rise to noncommuting matrices of size $n \geq 3$.

Example 2. Consider the abelian group $(\mathbb{Z}/n\mathbb{Z}, +)$. We can define a multiplication on $\mathbb{Z}/n\mathbb{Z}$ by declaring that $(a + n\mathbb{Z})(b + n\mathbb{Z}) = ab + n\mathbb{Z}$. We must check that this is well-defined. Given that $a + n\mathbb{Z} = c + n\mathbb{Z}$ and $b + n\mathbb{Z} = d + n\mathbb{Z}$, it follows that $a = c + ni$ and $b = d + nj$ for some integers i and j. Consequently, we have that $ab = (c + ni)(d + nj) = cd + n(cj + di + nij)$, from which we conclude that $(a + n\mathbb{Z})(b + n\mathbb{Z}) = ab + n\mathbb{Z} = cd + n\mathbb{Z} = (c + n\mathbb{Z})(d + n\mathbb{Z})$, as desired. Ultimately, we find that $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring. By Bézout's Theorem, the units of $\mathbb{Z}/n\mathbb{Z}$ are precisely the elements $a + n\mathbb{Z}$ such that $\gcd(n, a) = 1$ (hence, there are $\phi(n)$ units).

Consider the unique prime factorization $n = p_1 \cdots p_k$ for some (not necessarily distinct) primes p_i. Given that n is composite, it follows that $p_1 + n\mathbb{Z}$ and $p_2 \cdots p_k + n\mathbb{Z}$ are two nonzero elements of $\mathbb{Z}/n\mathbb{Z}$ such that $(p_1 + n\mathbb{Z})(p_2 \cdots p_k + n\mathbb{Z}) = p_1 \cdots p_k + n\mathbb{Z} = n + n\mathbb{Z} = 0 + n\mathbb{Z}$. Consequently, we refer to the elements $p_1 + n\mathbb{Z}$ and $p_2 \cdots p_k + n\mathbb{Z}$ as **zero divisors** of $\mathbb{Z}/n\mathbb{Z}$.

Generally, any nonzero element r of a ring R such that there exists a nonzero element s of R with $rs = 0_R$ is called a zero divisor. On the other hand, if we have that $rs = 0_R$ implies that $s = 0_R$, then we refer to r as a (left-)**regular** element of R. Essentially, an element r of R is (left-)regular if and only if it is (left-)cancellable, i.e., if and only if $rs = rt$ implies that $s = t$ for all elements s and t of R. Given that the only non-regular element of R is 0_R (equivalently, all nonzero elements of R are regular), we refer to R as a **domain**. Commutative domains are called **integral domains**.

Example 3. Observe that the integers $\mathbb{Z}$ form an integral domain that is not a (skew) field. Particularly, the only units in $\mathbb{Z}$ are ± 1 because $mn = 1$ if and only if $n = \frac{1}{m}$ (as rational numbers).

Example 2, Revisited. Given a prime p, we note that $\mathbb{Z}/p\mathbb{Z}$ is a commutative ring with p elements and $\phi(p) = p - 1$ units. Consequently, the only non-unit in $\mathbb{Z}/p\mathbb{Z}$ is the zero element $0 + p\mathbb{Z}$, hence every nonzero element of $\mathbb{Z}/p\mathbb{Z}$ is a unit. We say therefore that $\mathbb{Z}/p\mathbb{Z}$ is a (finite) **field**.

Example 3, Revisited. Observe that the rational numbers $\mathbb{Q}$ form a field: every nonzero element is of the form $\frac{r}{s}$ for some nonzero integers r and s with $\gcd(r, s) = 1$, and we have that $\frac{r}{s} \cdot \frac{s}{r} = 1$.

Proposition 2. If R is a field, then R is an integral domain.

Proof. Every nonzero element r of R is a unit, hence r^{-1} exists and satisfies $r^{-1}r = 1_R$. Consequently, if we have that $rs = 0_R$, then it follows that $s = 1_R s = r^{-1}rs = r^{-1}0_R = 0_R$,* as desired. □

Considering our examples so far, we have the following hierarchy of commutative rings.

$$\text{finite fields} \subsetneq \text{fields} \subsetneq \text{integral domains} \subsetneq \text{commutative rings}$$

Later, we will specialize this hierarchy to discuss different types of integral domains.

Proposition 3. If R is a finite integral domain, then R is a field.

Proof. Given any nonzero element x of R, consider the map $\varphi : R \to R$ defined by $\varphi(r) = rx$. By hypothesis that R is an integral domain, it follows that x is a regular (i.e., cancellable) element of R so that φ is injective: indeed, if we have that $\varphi(r) = \varphi(s)$, then $rx = sx$ implies that $r = s$. Considering that R is finite, it follows that φ is surjective (because an injective map between finite sets is a bijection), hence there exists a nonzero element y of R such that $xy = 1_R$. We conclude that x is a unit. But as x is arbitrary, it follows that every nonzero element of R is a unit. □

Q3, January 2016. Let k be a field, and let R be an integral domain such that $k \subseteq R$. Given that R is a finite-dimensional vector space over k, prove that R is a field.

Ring Homomorphisms

Given rings R and S, we say that a map $\varphi : R \to S$ is a **ring homomorphism** whenever we have that $\varphi(1_R) = 1_S$ and $\varphi(r + r') = \varphi(r) + \varphi(r')$ and $\varphi(rr') = \varphi(r)\varphi(r')$ for all elements r and r' of R. Put another way, φ is an additive group homomorphism from R to S that maps the multiplicative identity of R to the multiplicative identity of S and preserves the multiplication of R in S.

Remark 3. If R or S is a rng (i.e., it has no multiplicative identity), then it is not necessary to check that $\varphi(1_R) = 1_S$ because at least one of the elements 1_R or 1_S does not exist.

Given that there exists a ring homomorphism $\varphi : R \to S$, we say that S is an **R-algebra**. Every ring R is an algebra over itself via the identity homomorphism $\mathrm{id} : R \to R$ defined by $\mathrm{id}(r) = r$. Every ring homomorphism from a ring to itself is called a **ring endomorphism**.

Proposition 4. Consider the collection $\mathrm{End}(R) = \{\varphi : R \to R \,|\, \varphi \text{ is a ring homomorphism}\}$ of ring endomorphisms of R. We have that $\mathrm{End}(R)$ is a (noncommutative) ring under composition.

Proof. We leave the proof as an exercise for the reader. □

Example 4. Given a ring R, classify all ring homomorphisms $\varphi : \mathbb{Z} \to R$.

Proof. We leave the proof as an exercise for the reader. One consequence of this exercise is that $\mathbb{Z}$ is referred to as the initial object in the category of rings and ring homomorphisms. □

We refer to a bijective ring homomorphism as a **ring isomorphism**. Given that there exists a ring isomorphism $\varphi : R \to S$, we say that the rings R and S are **isomorphic**, and we write $R \cong S$. Like with groups, a bijective ring endomorphism is called a **ring automorphism**. Given a ring homomorphism $\varphi : R \to S$, we refer to the set $\ker \varphi = \{r \in R \,|\, \varphi(r) = 0_S\}$ as the **kernel** of φ.

Proposition 5. A ring homomorphism $\varphi : R \to S$ is injective if and only if $\ker \varphi = \{0_R\}$.

Proof. Considering that φ is an abelian group homomorphism, this follows from Proposition 3 from the notes on "Groups, Group Actions, and the Class Equation." □

Proposition 6. Given a ring homomorphism $\varphi : R \to S$, we have that $\ker \varphi$ is a subrng of R that is closed under (left- and right-)multiplication by elements of R.

Proof. Certainly, if 1_R is in $\ker\varphi$, then φ is the zero map, i.e., we have that $\ker\varphi = R$:

$$\varphi(r) = \varphi(r \cdot 1_R) = \varphi(r)\varphi(1_R) = \varphi(r)0_S = 0_S$$

for all elements r of R by Corollary 1. Consequently, we may assume that $\ker\varphi$ does not contain 1_R; we will show that $\ker\varphi$ is a subrng. By the subring test, it suffices to show that $\ker\varphi$ is closed under subtraction and multiplication. Given any two elements r and s of $\ker\varphi$, we have that

$$\varphi(r-s) = \varphi(r) - \varphi(s) = 0_S - 0_S = 0_S \text{ and } \varphi(rs) = \varphi(r)\varphi(s) = 0_S 0_S = 0_S,$$

hence $\ker\varphi$ is a subrng. Further, $\ker\varphi$ is closed under (left- and right-)multiplication by elements of R by the above displayed equation (if either r or s is in $\ker\varphi$, then rs is in $\ker\varphi$). □

We refer to a subrng I of R that is closed under multiplication by elements of R as a (two-sided) **ideal** of R. Often, we will deal with commutative rings, hence a two-sided ideal is simply an ideal, but in the case that R is noncommutative, we distinguish between left- and right-ideals. Observe that a proper ideal I of R cannot contain the multiplicative identity of R: if 1_R is in I, then by definition, we have that $r = r \cdot 1_R$ is in I for all elements r of R so that $I = R$.

Example 5. Observe that $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for any integer n because for any integers r and s, we have that $nr - ns = n(r-s)$, $(nr)(ns) = n(nrs)$, and $s(nr) = n(rs)$ are elements of $n\mathbb{Z}$.

Like with groups, we may consider the ideal generated by a subset of elements of R.

Proposition 7. Given any elements $x_1, \ldots, x_n$ of a commutative ring R, we have that

$$(x_1, \ldots, x_n) \stackrel{\text{def}}{=} R\langle x_1, \ldots, x_n\rangle = \{r_1x_1 + \cdots + r_nx_n \,|\, r_i \in R \text{ for each integer } 1 \leq i \leq n\}$$

is an ideal of R. We refer to $(x_1, \ldots, x_n)$ as the **ideal generated by** $x_1, \ldots, x_n$. Given that $n = 1$, we refer to the ideal $(x_1) = x_1R$ as the **principal ideal** generated by x_1.

We say that a set of generators $\{x_1, \ldots, x_n\}$ of an ideal I is a **minimal generating set** whenever $\{x_1, \ldots, x_n\} \setminus \{x_i\}$ does not generate I for any integer $1 \leq i \leq n$. Put another way, if we delete one generator, we obtain a strictly smaller ideal than I. Given that an ideal I has a finite minimal generating set, we say that I is **finitely generated**. Consequently, we may define

$$\mu(I) = \inf\{n \geq 0 \,|\, \{x_1, \ldots, x_n\} \text{ is a minimal generating set of } I\}.$$

Later, we will concern ourselves with the minimal number of generators $\mu(I)$ of an ideal I, but for now, we leave the next example as an interesting motivational exercise to the reader.

Example 6. Prove that $\mathbb{Z}$ can be generated by an ideal with n elements for each integer $n \geq 1$.

Our next proposition establishes that the generators of an ideal are not unique; rather, they can be chosen strategically so that the presentation of the ideal is more simple.

Proposition 8. Let R be a commutative ring with a finitely generated ideal $I = (f_1, \ldots, f_n)$. Consider the ideal $J = (f_1, \ldots, u_1f_1 + \cdots + u_nf_n, \ldots, f_n)$ for some units $u_1, \ldots, u_n$ of R, i.e., the ideal of R generated by the elements of $\{f_1, \ldots, f_n, u_1f_1 + \cdots + u_nf_n\} \setminus \{f_i\}$. We have that $I = J$.

Proof. One immediately sees that $J \subseteq I$ because each of the generators of J is an element of I. Conversely, each of the generators f_j of I for $j \neq i$ is an element of J, hence it suffices to prove that f_i is in J. Observe that $u_i f_i = u_1 f_1 + \cdots + u_n f_n + \sum_{j \neq i}(-u_j) f_j$ is an element of J so that $f_i = 1_R f_i = (u_i^{-1} u_i) f_i = u_i^{-1}(u_i f_i)$ is in J. We conclude therefore that $I \subseteq J$. □

Example 7. Find the simplest possible generating set of the ideal $I = (2, 4, 6, 9)$ in $\mathbb{Z}$.

By the one-step subgroup test, it follows that an ideal I of R is a normal subgroup of the abelian group R, hence we have that R/I is an abelian group with respect to the addition defined by $(r + I) + (s + I) = (r + s) + I$. Consider the multiplication $(r + I)(s + I) = rs + I$ defined on R/I. We must check that this is well-defined. Given that $r + I = u + I$ and $s + I = v + I$, it follows that $r = u + i$ and $s = v + j$ for some elements i and j of I. Consequently, we have that

$$rs = (u + i)(v + j) = uv + uj + vi + ij.$$

By hypothesis that I is an ideal of R, it follows that uj, vi, and ij are in I so that $uj + vi + ij$ is in I. We conclude therefore that $(r + I)(s + I) = rs + I = uv + I = (u + I)(v + I)$, as desired. Ultimately, we conclude that R/I is the **quotient ring** of R with respect to I.

Proposition 9. Given a ring R, every two-sided ideal I of R is the kernel of a ring homomorphism from R. Conversely, the kernel of a ring homomorphism from R is a two-sided ideal.

Proof. Given a two-sided ideal I of R, we have that R/I is a ring with respect to the multiplication $(r + I)(s + I) = rs + I$. Consequently, we have a ring homomorphism $\pi : R \to R/I$ defined by $\pi(r) = r + I$. Observe that r is in $\ker \pi$ if and only if $r + I = 0 + I$ if and only if r is in I, i.e., $\ker \pi = I$. Proposition 4 shows that $\ker \varphi$ is a two-sided ideal for any ring homomorphism $\varphi : R \to S$. □

Proposition 10. A ring homomorphism $\varphi : k \to R$ from a field k is either injective or zero.

Proof. Given that φ is injective, we are done. Otherwise, there exists a nonzero element r in $\ker \varphi$. By hypothesis that k is a field, it follows that r^{-1} exists and satisfies $r^{-1} r = 1_R$. Considering that $\ker \varphi$ is an ideal, $1_R = r^{-1} r$ is in $\ker \varphi$. But this implies that $\ker \varphi = R$ so that φ is zero. □

Corollary 2. Given a field k, the zero ideal 0_k and k are the only ideals of k.

One of the most important facts about any algebraic structure is the following.

Theorem 1. (First Isomorphism Theorem) Given any rings R and S and a ring homomorphism $\varphi : R \to S$, there exists a ring isomorphism $\psi : R/\ker \varphi \to \varphi(R)$.

Proof. We must first demonstrate that $\varphi(R)$ is a subring of S. We leave this to the reader. Considering that $\ker \varphi$ is an ideal of R, we may view $R/\ker \varphi$ as a ring with multiplication defined by $(r + \ker \varphi)(s + \ker \varphi) = rs + \ker \varphi$, hence it suffices to find a ring isomorphism $\psi : R/\ker \varphi \to \varphi(R)$. Consider the map $\psi : R/\ker \varphi \to \varphi(R)$ defined by $\psi(r + \ker \varphi) = \varphi(r)$. We must establish that ψ is well-defined, i.e., we must show that if $r + \ker \varphi = s + \ker \varphi$, then $\psi(r + \ker \varphi) = \psi(s + \ker \varphi)$. By definition, we have that $r + \ker \varphi = s + \ker \varphi$ if and only if $r - s + \ker \varphi = 0_R + \ker \varphi$ if and only if $r - s$ is in $\ker \varphi$ if and only if $\varphi(r - s) = 0_S$ if and only if $\varphi(r) - \varphi(s) = 0_S$ if and only if $\varphi(r) = \varphi(s)$ if and only if $\psi(r + \ker \varphi) = \psi(s + \ker \varphi)$. We conclude that ψ is well-defined. By

hypothesis that φ is a ring homomorphism, it follows that ψ is a ring homomorphism, and ψ is clearly surjective, hence it suffices to show that ψ is injective. Observe that $r + \ker\varphi$ is in $\ker\psi$ if and only if $\varphi(r) = \psi(r + \ker\varphi) = 0_S$ if and only if r is in $\ker\varphi$ if and only if $r + \ker\varphi = 0_R + \ker\varphi$ implies that $\ker\psi$ is trivial so that ψ is injective, as desired. □

Theorem 2. (Second Isomorphism Theorem) Given a ring R with a subring S and an ideal I of R, we have that $(S + I)/I \cong S/(S \cap I)$ as quotient rings.

Proof. We must first demonstrate that $S + I = \{s + i \mid s \in S,\, i \in I\}$ is a subring of R such that I is an ideal of $S + I$. Consequently, the quotient ring $(S + I)/I$ is well-defined. We must then establish that $S \cap I$ is an ideal of S. We leave these details to the reader. Once this is accomplished, it suffices by the First Isomorphism Theorem to find a surjective ring homomorphism $\varphi : S \to (S + I)/I$ such that $\ker\varphi = S \cap I$. We leave it to the reader to verify that the map $\varphi(s) = s + I$ does the job. □

Theorem 3. (Third Isomorphism Theorem) Given a ring R with ideals I and J such that $I \subseteq J$, we have that $(R/I)/(J/I) \cong R/J$ as quotient rings.

Proof. We must first demonstrate that I is an ideal of the rng J and that J/I is an ideal of R/I. We leave these details to the reader. Once this is accomplished, it suffices by the First Isomorphism Theorem to find a surjective group homomorphism $\varphi : R/I \to R/J$ such that $\ker\varphi = J/I$. We leave it to the reader to verify that the map $\varphi(r + I) = r + J$ does the job. Considering that this map is defined on a quotient ring, we must also establish that this map is well-defined. □

Theorem 4. (Fourth Isomorphism Theorem) Given a ring R with an ideal I, there exists a one-to-one correspondence $\{\text{subrings of } R \text{ that contain } I\} \leftrightarrow \{\text{subrings of } R/I\}$ that sends $S \mapsto S/I$ for any subring S of R that contains I with the following properties.

1.) Given any subrings S and T of R such that $I \subseteq S$ and $I \subseteq T$, we have that $S \subseteq T$ if and only if $S/I \subseteq T/I$. Put another way, this bijection is inclusion-preserving.

2.) Given any subring J of R that contains the ideal I, we have that J is an ideal of R if and only if J/I is an ideal of R/I.

Ideals

Recall that a ring is an abelian group under addition in which there exists a notion of multiplication (that may not be commutative). Until now, we have seen that rings have exhibited many of the same properties as abelian groups, e.g., rings have homomorphisms between them; ideals are analogous to normal subgroups; quotient rings are analogous to quotient groups; and there four isomorphism theorems for rings that are analogous to the four isomorphism theorems for groups.

Our immediate aim is to impress that the multiplicative structure of a ring gives it a much richer theory than that of groups. We say that a proper ideal P of R with the property that rs is in P implies that either r is in P or s is in P for all elements r and s of R is **prime**.

Example 8. Consider the ideal $5\mathbb{Z}$ of $\mathbb{Z}$. Given any elements m and n of $\mathbb{Z}$ such that mn is in $5\mathbb{Z}$, by definition, we have that $mn = 5i$ for some integer i, from which it follows that $5 \mid mn$. Considering that 5 is a prime number, we must have that $5 \mid m$ or $5 \mid n$, hence $5\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. Ultimately, this example serves to show that prime ideals are a generalization of prime numbers.

Proposition 11. Given a ring R, an ideal P of R is prime if and only if R/P is a domain.

Proof. We will assume first that P is prime. We claim that R/P is a domain, i.e., all nonzero elements of R/P are regular. Given any nonzero elements $r+P$ and $s+P$ of R/P, consider the product $rs+P=(r+P)(s+P)$. On the contrary, if it were the case that $rs+P=0_R+P$, then we would have that rs is in P. By the primality of P, we would therefore have that either r is in P or s is in P so that either $r+P=0_R+P$ or $s+P=0_R+P$ — a contradiction. We conclude therefore that all nonzero elements of R/P are regular so that R is a domain.

Conversely, we will assume that R/P is a domain. Given any elements r and s in R such that rs in P, we have that $(r+P)(s+P)=rs+P=0_R+P$. By hypothesis that R/P is a domain, it follows that $r+P=0_R+P$ or $s+P=0_R+P$ so that r is in P or s is in P, i.e., P is prime. □

Corollary 3. There exist ideals that are not prime.

Proof. Consider the ideal $4\mathbb{Z}$ of $\mathbb{Z}$. By Example 2, the element $2+4\mathbb{Z}$ of $\mathbb{Z}/4\mathbb{Z}$ is a zero divisor, hence $\mathbb{Z}/4\mathbb{Z}$ is not a domain. By Proposition 11, therefore, $4\mathbb{Z}$ is not a prime ideal of $\mathbb{Z}$. □

Example 8, Revisited. Consider the ideal $5\mathbb{Z}$ of $\mathbb{Z}$. Given any ideal $n\mathbb{Z}$ of $\mathbb{Z}$ such that $5\mathbb{Z}\subseteq n\mathbb{Z}$, it follows that we may write $5=ni$ for some integer i (because $5\cdot 1$ is in $5\mathbb{Z}$). But this implies that $n\,|\,5$ so that $n=1$ or $n=5$. Consequently, we have that $n\mathbb{Z}=5\mathbb{Z}$ or $n\mathbb{Z}=1\mathbb{Z}=\mathbb{Z}$.

We say that a proper ideal M of a ring R is **maximal** if it has the property that $M\subseteq N$ for some ideal N of R implies that $N=M$ or $N=R$. Put another way, a maximal ideal M is the largest (with respect to inclusion) proper ideal of R that contains M.

Proposition 12. Given a ring R, an ideal M of R is maximal if and only if R/M is a field.

Proof. We will assume first that M is maximal. We claim that R/M is a field, i.e., all nonzero elements of R/M are units. Given any nonzero element $r+M$ of R/M, we must produce an element $s+M$ of R/M such that $rs+M=(r+M)(s+M)=1_R+M$. Put another way, we must produce an element s of $R-M$ such that $rs-1_R=m$ for some element m of M. Consider the ideal

$$N=M+rR=\{m+rs\,|\,m\in M \text{ and } s\in R\}.$$

Given any element m of M, we have that $m=m+r0_R$ is in N so that $M\subseteq N$. Considering that $r=0_R+r1_R$ is in N and not in M (because $r+M$ is nonzero), it follows that $M\neq N$. By the maximality of M, we have therefore that $N=R$ so that $1_R=m+rs$ for some element s of R. We claim that s is not in M. For if it were in M, then rs would be in m so that $1_R=m+rs$ would be in M, and ultimately, we would have that $M=R$ — a contradiction. Consequently, we must have that s is not in M so that $s+M$ is nonzero. Further, it follows from the identity $rs-1_R=-m$ that $rs-1_R=0_R+M$ so that $(r+M)(s+M)=rs+M=1_R+M$, as desired.

Conversely, we will assume that R/M is a field. By the Fourth Isomorphism Theorem, we have that $M\subseteq N$ for some ideal N of R if and only if $N/M\subseteq R/M$. By Corollary 1, the only ideals of a field are the zero ideal and the field itself, hence we have that $N/M=\{0_R+M\}$ or $N/M=R/M$. But this implies that $N=M$ or $N=R$, hence M is maximal, as desired. □

Corollary 4. Every maximal ideal is prime, but there exist prime ideals that are not maximal.

Proof. By Proposition 12, given a maximal ideal M of a ring R, we have that R/M is a field. Consequently, every nonzero element of R/M is a unit and must therefore be regular. (Why?) We conclude that R/M is a domain, hence by Proposition 11, it follows that M is prime.

On the other hand, given a field k, consider the set $k[x, y]$ of polynomials in the variables x and y with coefficients in k. Observe that $k[x, y]$ is a commutative ring with multiplicative identity 1_k and additive identity 0_k. By Proposition 9, an ideal I of $k[x, y]$ is the kernel of a ring homomorphism from $k[x, y]$. Consider the map $\varphi : k[x, y] \to k[x]$ defined by $\varphi(p(x, y)) = p(x, 0)$. Because a polynomial in $k[x, y]$ can be viewed as a function from k^2 to k, it follows that φ is a ring homomorphism. Consequently, $\ker \varphi$ is an ideal of $k[x, y]$. Observe that $k[x]$ is a domain, but the variable x is not a unit, hence $k[x]$ is not a field. We conclude that $\ker \varphi$ is a prime ideal that is not maximal. □

Q1a, January 2018. Consider the ring $R = \mathbb{C}[x, y, z]$. Prove that $I = (x, y)$ is a prime ideal in R.

Q5, August 2019. Consider the ring $R = \mathbb{Q}[x, y, z]/I$, where $I = (x^2y - z^5)$.

(a.) Prove that R is not a field. Determine with proof whether R is a domain.

(b.) Determine with proof whether $J = (\bar{x}, \bar{y})$ is a prime ideal of R.

Considering our examples so far, we have the following hierarchy of ideals.

$$\text{maximal ideals} \subsetneq \text{prime ideals} \subsetneq \text{ideals}$$

We will now discuss how to construct new ideals from old. Given some ideals I and J of a ring R as sets, it is natural to consider the sets $I \cup J$ and $I \cap J$. Considering that I and J are also subrngs of R, we may also consider $I + J = \{i + j \,|\, i \in I,\, j \in J\}$ and $IJ = \{\sum_{k=1}^{n} i_k j_k \,|\, i_k \in I,\, j_k \in J\}$.

Example 9. Let R be a ring with (two-sided) ideals I and J. Prove that the set $I * J = \{ij \,|\, i \in I,\, j \in J\}$ of products of element an in I and an element of J is not an ideal of R.

Proposition 13. Given any ideals I and J of a ring R, we have that $I \cap J$, $I + J$, and IJ are ideals of R with $IJ \subseteq I \cap J \subseteq I, J \subseteq I + J$; however, the set $I \cup J$ is not generally an ideal.

Proof. We leave it as an exercise to the reader to prove that $I \cap J$, $I + J$, and IJ are ideals of R. Once this is established, consider an element $\sum_{k=1}^{n} i_k j_k$ of IJ. By hypothesis that I and J are (two-sided) ideals of R, it follows that $i_k j_k$ is in I because i_k is in I and j_k is in R and $i_k j_k$ is in J because i_k is in R and j_k is in J for each integer $1 \leq k \leq n$. We conclude that $IJ \subseteq I \cap J$. Certainly, we have that $I \cap J \subseteq I$ and $I \cap J \subseteq J$. Last, for any element i of I, we have that $i = i + 0_R$ is in $I + J$ because J is a subrng of R. We have therefore that $I \subseteq I + J$ and likewise $J \subseteq I + J$.

Let I and J be distinct proper nontrivial ideals of R. On the contrary, we will assume that $I \cup J$ is an ideal of R. Consequently, $I \cup J$ is a subrng of R and hence must be closed under subtraction. Given any nonzero element i of $I \setminus J$ and j of $J \setminus I$, we must therefore have that $i - j$ is in $I \cup J$. But this implies that either $i - j \in I$ so that $j \in I$ or $i - j \in J$ so that $i \in J$ — a contradiction. □

Corollary 5. Let R be a ring with finitely generated ideals $I = (x_1, \ldots, x_m)$ and $J = (y_1, \ldots, y_n)$. We have that $IJ = (x_i y_j \,|\, 1 \leq i \leq m \text{ and } 1 \leq j \leq n)$. Put another way, the product of two finitely generated ideals I and J is finitely generated by the products of the generators of I and J.

Proof. By Proposition 13, it follows that IJ is an ideal of R. Given any element $i \in I$ and $j \in J$, we have that $i = r_1x_1 + \cdots + r_mx_m$ and $j = s_1y_1 + \cdots + s_ny_n$. Consequently, we find that

$$ij = (r_1x_1 + \cdots + r_mx_m)(s_1y_1 + \cdots + s_ny_n) = \sum_{i=1}^{m}\sum_{j=1}^{n} r_is_jx_iy_j$$

is an element of $(x_iy_j \,|\, 1 \leq i \leq m \text{ and } 1 \leq j \leq n)$. Consequently, each of the elements in the sum $\sum_{k=1}^{n} i_kj_k$ is in $(x_iy_j \,|\, 1 \leq i \leq m \text{ and } 1 \leq j \leq n)$, hence we find that $IJ \subseteq (x_iy_j \,|\, 1 \leq i \leq m \text{ and } 1 \leq j \leq n)$. Conversely, for any integers $1 \leq i \leq m$ and $1 \leq j \leq n$, we have that $x_i \in I$ and $y_j \in J$ so that $x_iy_j \in IJ$. Considering that IJ is an ideal of R, it follows that every R-linear combination of elements x_iy_j for some integers $1 \leq i \leq m$ and $1 \leq j \leq n$ so that $(x_iy_j \,|\, 1 \leq i \leq m \text{ and } 1 \leq j \leq n) \subseteq IJ$. □

Our next proposition reasserts that prime ideals function analogously to prime integers.

Proposition 14. Given a prime ideal P of a ring R and ideals I and J of R such that $IJ \subseteq P$, we have that $I \subseteq P$ or $J \subseteq P$.

Proof. We may assume that $J \nsubseteq P$ and subsequently establish that $I \subseteq P$.* Given any element $i \in I$, we have that $ij \in P$ for every element $j \in J$ by hypothesis that $IJ \subseteq P$. Considering that $J \nsubseteq P$, there exists an element $j_0 \in J$ such that $j_0 \notin P$. By the primality of P and the fact that $ij_0 \in P$, we must have that $i \in P$. We conclude therefore that $I \subseteq P$, as desired. □

*Convince yourself that for some statements A, B, and C, there is a logical equivalence

$$(A \implies (B \vee C)) \iff ((A \wedge \neg C) \implies B).$$

Q2, August 2018. For each of the following claims, provide a proof or an explicit counterexample.

(a.) Consider the ring A of continuous functions $f : (0, 1) \to \mathbb{R}$ with ideal $I_\alpha = \{f \in A \,|\, f(\alpha) = 0\}$.

(i.) I_α is a maximal ideal.

(ii.) $I_{1/2} \cap I_{\pi/4}$ is a prime ideal.

(iii.) (0) is a prime ideal.

(c.) $(\bar{x})$ is a prime ideal in $R = \mathbb{C}[x, y]/(xy)$.

Q5c, August 2019. Consider the ring $R = \mathbb{Q}[x, y, z]/I$, where $I = (x^2y - z^5)$. Prove that for the ideal $J = (\bar{x}, \bar{y})$ of R, we have that $\bar{z}^5 \in J^2$ and yet $\bar{z}^4 \notin J^2$.

Proposition 15. Given an ascending chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ of ideals of a ring R, we have that $\cup_{n=1}^{\infty} I_n$ is an ideal of R.

Proof. It suffices to show that $\cup_{n=1}^{\infty} I_n$ is closed under subtraction and multiplication by elements of R. We leave the details as an exercise for the reader. □

Q2, August 2013. Consider an integral domain R and a collection $\{P_n\}_{n=1}^{\infty}$ of prime ideals.

(a.) Prove that if $P_1 \supseteq P_2 \supseteq P_3 \supseteq \cdots$, then $\cap_{n=1}^{\infty} P_n$ is a prime ideal.

(b.) Give an explicit counterexample to part (a.) when the primes do not form a descending chain.

Our next two propositions show that every ring possesses at least one maximal ideal, and moreover, that maximal ideals are actually ubiquitous in a commutative ring. We note that the ideas contained in the proofs are quite common in commutative algebra. We first need a technical lemma.

Theorem 5. (Zorn's Lemma) Every partially ordered set S with the property that every chain in S has an upper bound in S contains at least one maximal element.

Proposition 16. Every nonzero ring possesses a maximal ideal.

Proof. Consider the collection $S = \{I \subsetneq R \,|\, I \text{ is an ideal of } R\}$ of proper ideals of R. Observe that S is partially ordered by set inclusion, and it is nonempty because it contains the zero ideal $\{0_R\}$. Consequently, we seek to employ Zorn's Lemma. Consider a chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ of ideals in S. By Proposition 15, it follows that $\cup_{n=1}^{\infty} I_n$ is an ideal of R. Further, it is a proper ideal: if it were the case that $1_R \in \cup_{n=1}^{\infty} I_n$, then we would have that $1_R \in I_n$ for some integer $n \geq 1$ so that $I_n = R$ — a contradiction to our assumption that I_n is a proper ideal of R. Ultimately, we have established that every chain in S has an upper bound in S, hence S has a maximal element. By definition, this maximal (with respect to inclusion) element is a maximal ideal of R. □

Proposition 17. Every proper ideal of a nonzero ring is contained in a maximal ideal.

Proof. Given an ideal $I \subsetneq R$, consider the collection $S = \{J \subsetneq R \,|\, J \text{ is an ideal of } R \text{ and } I \subseteq J\}$ of proper ideals of R that contain I. We leave it as an exercise to the reader to establish that there exists a maximal element M of S. (Use Zorn's Lemma.) By definition, we have that M is a maximal ideal of R that contains I. (One other way to see it is that if N is a proper ideal of R that strictly contains M, then by hypothesis, N cannot contain I. But then, the sum $I + N$ is an ideal of R that contains I and M, hence we must have that $I + N = R$ so that M is maximal.) □

Q4, January 2014. Consider a commutative ring R with distinct maximal ideals M_1 and M_2.

(a.) Prove that for any integer $n \geq 1$, we have that $R = M_1^n + M_2^n$, where M_i^n denotes the ideal consisting of all finite sums of n-fold products of elements in M_i.

(b.) Consider the polynomial ring $\mathbb{R}[x, y]$. Given a positive integer $n \geq 1$ and two distinct points $P_1 = (a_1, b_1)$ and $P_2 = (a_2, b_2)$ in $\mathbb{R}^2$, prove that for each $f(x, y) \in \mathbb{R}[x, y]$, there exist $g(x, y)$ and $h(x, y)$ in $\mathbb{R}[x, y]$ such that

(i.) $f(x, y) = g(x, y) + h(x, y)$;

(ii.) $g(x, y)$ and all of its partial derivatives of order $< n$ vanish at P_1; and

(iii.) $h(x, y)$ and all of its partial derivatives of order $< n$ vanish at P_2.

Q2, January 2017. Given an integral domain R, assume that there exists a nonzero, non-unit a in R such that for every element r in R, there exists a unit u and a non-negative integer n with $r = ua^n$. We say in this case that R is a **discrete valuation ring**.

(a.) Prove that $P = aR$ is the unique maximal ideal of R.

(b.) Prove that $\cap_{n=1}^{\infty} P^n = (0_R)$.

(c.) Prove that $R\left[\frac{1}{a}\right] = \left\{r_n \frac{1}{a^n} + \cdots + r_1 \frac{1}{a} + r_0 \,|\, r_0, r_1, \ldots, r_n \in R \text{ and } n \geq 0\right\}$ is a field.

The Chinese Remainder Theorem

One of the most celebrated theorems in number theory remains the Chinese Remainder Theorem. Our aim in this section is to generalize the Chinese Remainder Theorem to a statement about rings and ideals. Ultimately, it will be shown that the Chinese Remainder Theorem from number theory is a consequence of the Chinese Remainder Theorem for commutative rings as applied to $R = \mathbb{Z}$.

Theorem 6. Let R be a commutative ring with pairwise **comaximal** ideals $I_1, \ldots, I_n$, i.e., ideals $I_1, \ldots, I_n$ that satisfy $I_i + I_j = R$ whenever i and j are distinct. We have that

(i.) $\dfrac{R}{I_1 \cap \cdots \cap I_n} \cong \dfrac{R}{I_1} \times \cdots \times \dfrac{R}{I_n}$ and

(ii.) $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$.

Proof. We proceed by induction on the number n of pairwise comaximal ideals. Given that $n = 2$, consider the ring homomorphism $\varphi : R \to (R/I_1) \times (R/I_2)$ defined by $\varphi(r) = (r + I_1, r + I_2)$. We claim that φ is surjective, hence by the First Isomorphism Theorem, we have that

$$\frac{R}{I_1} \times \frac{R}{I_2} \cong \frac{R}{\ker \varphi}.$$

Observe that r is in $\ker \varphi$ if and only if $r + I_1 = 0 + I_1$ and $r + I_2 = 0 + I_2$ if and only if r is in I_1 and r is in I_2 if and only if r is in $I_1 \cap I_2$, hence we have that $\ker \varphi = I_1 \cap I_2$, as desired.

We will establish now that φ is surjective. Given any elements $r + I_1$ and $s + I_2$, we wish to find an element t of R such that $\varphi(t) = (r + I_1, s + I_2)$. By hypothesis that I_1 and I_2 are comaximal, we have that $I_1 + I_2 = R$ so that $1_R = i + j$ for some elements i of I_1 and j of I_2. Consequently, we may write $r = ri + rj$ and $s = si + sj$ so that on the level of cosets, we have that

$$r + I_1 = ri + rj + I_1 = 0_R + rj + I_1 = rj + I_1 \text{ and}$$
$$s + I_2 = si + sj + I_2 = si + 0_R + I_2 = si + I_2.$$

But this implies that $t = rj + si$ satisfies $\varphi(t) = (r + I_1, s + I_2)$ so that φ is surjective.* By Proposition 13, we have that $I_1 I_2 \subseteq I_1 \cap I_2$, hence it suffices to show that $I_1 \cap I_2 \subseteq I_1 I_2$. Every element x of $I_1 \cap I_2$ can be written as $x = 1_R x = (i + j)x = ix + xj$ for some i in I_1 and j in I_2. Considering that ix is in $I_1 I_2$ and jx is in $I_1 I_2$, it follows that $x = ix + jx$ is in $I_1 I_2$ (because $I_1 I_2$ is an ideal).

We will assume inductively that the claim holds for some integer $n \geq 3$. Consider the map

$$\varphi : R \to \frac{R}{I_1 \cdots I_{n-1}} \times \frac{R}{I_n}$$

defined by $\varphi(r) = (r + I_1 \cdots I_{n-1}, r + I_n)$. By induction, it suffices to show that φ is surjective and $\ker \varphi = I_1 \cdots I_{n-1} \cap I_n$. Considering that I_i and I_n are comaximal for all integers $1 \leq i \leq n - 1$, it follows that $I_i + I_n = R$ for all integers $1 \leq i \leq n - 1$. Consequently, there exist elements $i_1, \ldots, i_{n-1}, j_1, \ldots, j_{n-1}$ such that $i_k + j_k = 1_R$, $i_k \in I_k$, and $j_k \in I_n$ for each integer $1 \leq k \leq n - 1$. By taking the product of all of these sums, we obtain an element i of $I_1 \cdots I_{n-1}$ and j of I_n such that $i + j = 1_R$.** By the second paragraph above, this is sufficient to prove that φ is surjective. $\square$

*Explicitly, we have that

$$\varphi(t) = \varphi(rj + si) = (rj + si + I_1, rj + si + I_2) = (rj + I_1, si + I_2) = (r + I_1, s + I_2).$$

**Observe that

$$(i_1 + j_1) \cdots (i_{n-1} + j_{n-1}) = i_1 \cdots i_{n-1} + j_1 \cdots j_{n-1} + \text{other terms},$$

where the quantity "other terms" involves products of things in I_k and I_n — a subset of I_n. Consequently, we may take $i = i_1 \cdots i_{n-1}$ and $j = j_1 \cdots j_{n-1} + \text{other terms}$.

We note that the first property of the Chinese Remainder Theorem holds for two-sided ideals of any (not necessarily commutative) ring; however, as the proof bears out, the second property does not hold in general for noncommutative rings (as it requires some product to commute).

Corollary 6. Let R be a commutative ring. Every pair of distinct maximal ideals of R are comaximal. Further, the intersection of any two distinct maximal ideals is the product of those ideals.

Proof. Consider any pair of distinct maximal ideals M_1 and M_2 of R. By Proposition 13, we have that $M_1 + M_2$ is an ideal of R that contains M_1 (and M_2). By the maximality of M_1 (or M_2), we conclude that $M_1 + M_2 = R$, hence M_1 and M_2 are comaximal. By the Chinese Remainder Theorem, therefore, we have that $M_1 \cap M_2 = M_1 M_2$, as desired. □

Q2b, August 2010. Consider the polynomial ring $\mathbb{Z}[x]$. Given that the ideals $M_1 = (3, x^2 + x + 2)$ and $M_2 = (2, x^2 + x + 1)$ of $\mathbb{Z}[x]$ are maximal, find with proof a set of generators for $M_1 \cap M_2$.

Extension and Contraction of Ideals

Let R and S be commutative rings. Recall that if there exists a ring homomorphism $\varphi : R \to S$, we refer to S as an R-algebra. Of course, one might naturally wonder what becomes of the image $\varphi(I)$ of an ideal I of R under the ring homomorphism φ. One of the most immediate examples of an R-algebra is the polynomial ring $R[x]$ over any commutative ring R: in this case, the map $\iota : R \to R[x]$ is simply the inclusion map $\iota(r) = r$ (considered as the constant polynomial). Observe that for the ring of integers $\mathbb{Z}$, the image of the ideal $2\mathbb{Z}$ under the inclusion map $\iota : \mathbb{Z} \to \mathbb{Z}[x]$ is no longer an ideal. Explicitly, we have that $\iota(2\mathbb{Z})$ consists of all integer multiples of 2, hence the element $2x$ is not in $\iota(2\mathbb{Z})$, from which it follows that $\iota(2\mathbb{Z})$ is not an ideal of $\mathbb{Z}[x]$ (as it is not closed under multiplication by ring elements). Consequently, we may clear up this problem by defining the **extension** of $2\mathbb{Z}$ in $\mathbb{Z}[x]$ to be the ideal $2\mathbb{Z}^e = \iota(2\mathbb{Z})\mathbb{Z}[x]$ generated by $\iota(2\mathbb{Z})$ in $\mathbb{Z}[x]$. Generally, for an ideal I of a ring R, the extension of I via the ring homomorphism $\varphi : R \to S$ is the ideal generated by the image $\varphi(I)$ of I under φ in S, i.e., we have that $I^e = \varphi(I)S$.

Proposition 18. Given a surjective ring homomorphism $\varphi : R \to S$ of commutative rings and an ideal I of R, we have that $\varphi(I)$ is an ideal of S — namely, we have that $\varphi(I) = I^e$.

Proof. We will prove first that $\varphi(I)$ is an ideal of S. By the subrng test, it suffices to show that $\varphi(I)$ is closed under subtraction and multiplication by elements of S. Given any two elements $\varphi(i)$ and $\varphi(j)$ in $\varphi(I)$, we have that $\varphi(i) - \varphi(j) = \varphi(i - j)$. Considering that I is an ideal of R, it follows

that $i-j$ is in I so that $\varphi(i)-\varphi(j)=\varphi(i-j)$ is in $\varphi(I)$. Given any element s of S, there exists an element r of R such that $s=\varphi(r)$ by hypothesis that φ is surjective. Consequently, we have that $s\varphi(i)=\varphi(r)\varphi(i)=\varphi(ri)$. Considering that I is an ideal of R, it follows that ri is in I so that $s\varphi(i)=\varphi(ri)$ is in $\varphi(I)$. We conclude that $\varphi(I)$ is an ideal of S. By hypothesis that φ is surjective, we have that $S=\varphi(R)$ so that $I^e=\varphi(I)S=\varphi(I)\varphi(R)=\varphi(IR)=\varphi(I)$, as desired. □

Remark 4. Prime ideals do not necessarily extend to prime ideals.

Proof. Consider the set $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\,|\,a,b\in\mathbb{Z}\}\subseteq\mathbb{R}$. By the subring test, it suffices to prove that $\mathbb{Z}[\sqrt{2}]$ is closed under subtraction and multiplication and contains the multiplicative identity 1 of $\mathbb{R}$. We leave these details to the reader. Once that is accomplished, we may consider the ring homomorphism $\iota:\mathbb{Z}\to\mathbb{Z}[\sqrt{2}]$ defined by $\iota(n)=n+0\sqrt{2}$. Observe that the ideal $2\mathbb{Z}$ of $\mathbb{Z}$ is prime (because 2 is a prime integer); however, considering that $2=\sqrt{2}\cdot\sqrt{2}=(0+1\cdot\sqrt{2})(0+1\cdot\sqrt{2})$ in $\mathbb{Z}[\sqrt{2}]$ and $\sqrt{2}$ is not an element of $2\mathbb{Z}^e=\iota(2\mathbb{Z})\mathbb{Z}[\sqrt{2}]$ in $\mathbb{Z}[\sqrt{2}]$, it follows that $2\mathbb{Z}^e$ is not prime. □

Our proof also establishes that maximal ideals do not necessarily extend to maximal ideals because every maximal ideal is prime by Corollary 4.

Conversely, one might naturally wonder what can be said of the preimage of an ideal J of S under the commutative ring homomorphism $\varphi:R\to S$. We cut right to the chase.

Proposition 19. Given a ring homomorphism $\varphi:R\to S$ of commutative rings and an ideal J of S, we have that $\varphi^{-1}(J)=\{r\in R\,|\,\varphi(r)\in J\}$ is an ideal of S. We refer to the ideal $\varphi^{-1}(J)$ as the **contraction** of J via φ, and we write $\varphi^{-1}(J)=J^c$.

Proof. By the subrng test, it suffices to show that J^c is closed under subtraction and multiplication by elements of R. By definition, given any elements r and s of J^c, we have that $\varphi(r)$ and $\varphi(s)$ are in J. By hypothesis that J is an ideal of S, we have that $\varphi(r+s)=\varphi(r)+\varphi(s)$ is in J so that $r+s$ is in J^c. Given any element t of R, we have that $\varphi(t)$ is in S. Considering that J is an ideal of S and r is in J^c, it follows that $\varphi(t)\varphi(r)=\varphi(tr)$ is in J so that tr is in J^c. □

Proposition 20. Contractions of prime ideals are prime.

Proof. Let P be a prime ideal of S. Consider some elements r and s of P^c such that rs is in P^c. By definition, we have that $\varphi(r)\varphi(s)=\varphi(rs)$ is in P. By the primality of P, therefore, we have that $\varphi(r)$ is in P or $\varphi(s)$ is in P so that r is in P^c or s is in P^c, as desired. □

Later, when we the integral closure of a ring, we will say more about contractions of ideals.

Oka Families of Ideals

Given any two ideals I and J of a commutative ring R, consider the set

$$(I:_R J)=\{r\in R\,|\,rj\in I\text{ for all }j\in J\}=\{r\in R\,|\,rJ\subseteq I\}.$$

Proposition 21. We have that $(I:_R J)$ is an ideal of R called the **colon ideal** of I and J.

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

Before moving on to the main topic of this section, we note that there are many interesting properties to explore involving the colon of two ideals. For instance, one should prove the following.

Proposition 22. Let I, J, and K be ideals of a commutative ring R.

(i.) We have that $I \subseteq (I :_R J)$, $(I :_R R) = I$, and $(R :_R I) = R$.

(ii.) We have that $(I :_R J)J \subseteq I$. Equality holds if and only if J is principal and $I \subseteq J$.

(iii.) We have that $((I :_R J) :_R K) = (I :_R JK) = ((I :_R K) :_R J)$.

(iv.) For any ideals $\{I_\alpha\}_{\alpha \in A}$ of R, we have that $((\cap_{\alpha \in A} I_\alpha) :_R J) = \cap_{\alpha \in A}(I_\alpha :_R J)$.

(v.) For any ideals $\{J_\alpha\}_{\alpha \in A}$ of R, we have that $(I :_R \sum_{\alpha \in A} J_\alpha) = \cap_{\alpha \in A}(I :_R J_\alpha)$.

Consider a family $\mathfrak{F}$ of ideals of a commutative ring R. We say that $\mathfrak{F}$ is **Oka** whenever

(a.) R is an ideal of $\mathfrak{F}$ and

(b.) for any ideal I of R and any element x of R,

(i.) $I + xR$ is in $\mathfrak{F}$ and

(ii.) $(I :_R xR)$ is in $\mathfrak{F}$

together imply that I is in $\mathfrak{F}$.

Our next proposition illustrates the importance and usefulness of Oka families of ideals.

Proposition 23. Let $\mathfrak{F}$ be an Oka family of ideals of a commutative ring R. An ideal I of R that is maximal (with respect to inclusion) with respect to the property that I is not in $\mathfrak{F}$ is prime.

Proof. Let I be an ideal of R that is maximal (with respect to inclusion) with respect to the property that I is not in $\mathfrak{F}$. We will establish that if x and y are any elements of R such that xy is in I, then either x is in I or y is in I. On the contrary, let us assume that neither x nor y is in I. Consequently, the ideal $I + xR$ strictly contains I. By hypothesis that I is maximal (with respect to inclusion) with respect to the property that I is not in $\mathfrak{F}$, it follows that $I + xR$ is in $\mathfrak{F}$. By property (i.) of Proposition 22, we have that $I \subseteq (I :_R xR)$. If these ideals were equal, then y would be in I (because xy is in I so that y is in $(I :_R xR) = I$) — a contradiction. Consequently, the ideal $(I :_R xR)$ strictly contains I, and as before, it follows that $(I :_R xR)$ is in $\mathfrak{F}$. But by assumption that $\mathfrak{F}$ is an Oka family, it follows that I is in $\mathfrak{F}$ — a contradiction. We conclude that x is in I or y is in I. □

One immediate consequence of Proposition 23 is that we can generate prime ideals of commutative rings by recognizing a collection of ideals as an Oka family $\mathfrak{F}$ and finding the largest (with respect to inclusion) ideal that is not contained in $\mathfrak{F}$. We demonstrate this idea as follows.

Corollary 7. Let R be a commutative ring. Every maximal (with respect to inclusion) element of $\{I \subseteq R \,|\, I \text{ is an ideal, and } I \text{ is not principal}\}$ is prime.

Proof. We will establish that $\mathfrak{F} = \{I \subseteq R \,|\, I \text{ is a principal ideal}\}$ is an Oka family. By Proposition 23, therefore, any ideal that is maximal (with respect to inclusion) with respect to the property that it is not in $\mathfrak{F}$ is prime. Put another way, every maximal (with respect to inclusion) element of $\{I \subseteq R \,|\, I \text{ is an ideal, and } I \text{ is not principal}\}$ is prime, as desired.

Of course, we have that $R = 1_R R$ is a principal ideal, hence R is in $\mathfrak{F}$. Consider an ideal I of R and any element x of R such that $I + xR$ is in $\mathfrak{F}$ and $(I :_R xR)$ is in $\mathfrak{F}$. We claim that I is in $\mathfrak{F}$. Considering that $I + xR$ and $(I :_R xR)$ are in $\mathfrak{F}$, by definition, we have that $I + xR = aR$ and $(I :_R xR) = bR$ for some elements a and b of R. By property (v.) of Proposition 22, we have that $(I :_R I + xR) = (I :_R I) \cap (I :_R xR) = R \cap (I :_R xR) = (I :_R xR) = bR$. By property (ii.) of Proposition 22, we have that $I = (I :_R I + xR)(I + xR)$ because $I + xR$ is principal by hypothesis and $I \subseteq I + xR$ (by Proposition 13). We conclude therefore that

$$I = (I :_R I + xR)(I + xR) = (I :_R xR)(I + xR) = (bR)(aR) = (ab)R$$

is principal. Put another way, we have that I is in $\mathfrak{F}$, hence $\mathfrak{F}$ is an Oka family. □

Corollary 8. Let R be a commutative ring. If every prime ideal of R is principal, then every ideal of R is principal.

Proof. We prove the contrapositive, i.e., we will assume that there exists a non-principal ideal of R, and we will show that there exists a prime non-principal ideal of R. By hypothesis, the collection $\mathcal{N} = \{I \subseteq R \,|\, I \text{ is an ideal, and } I \text{ is not principal}\}$ is nonempty. Certainly, it is partially ordered by inclusion. By Zorn's Lemma, if every chain of elements of $\mathcal{N}$ has an upper bound in $\mathcal{N}$, then there exists a maximal (with respect to inclusion) element of $\mathcal{N}$ that is prime by Corollary 5.

Consider a chain $I_1 \subseteq I_2 \subseteq \cdots$ of elements of $\mathcal{N}$. By Proposition 15, the set $\cup_{n=1}^{\infty} I_n$ is an ideal of R. On the contrary, if it were principal, then there would exist an element x of R such that $\cup_{n=1}^{\infty} I_n = xR$. Considering that $x = x \cdot 1_R$ is in $xR = \cup_{n=1}^{\infty}$, it follows that x is in I_n for some integer $n \geq 1$. But then, we have that xr is in I_n for every element r of R by hypothesis that I_n is an ideal of R, from which it follows that $xR \subseteq I_n \subseteq \cup_{n=1}^{\infty} I_n \subseteq xR$ so that $I_n = xR$ is principal — a contradiction. We conclude that $\cup_{n=1}^{\infty} I_n$ is not principal so that $\cup_{n=1}^{\infty} I_n$ is in $\mathcal{N}$, as desired. □

Later, we shall see that the structure of prime ideals of rings with certain properties determines the structure of all ideals of that ring in a similar fashion to Corollary 8.

Noetherian Rings

Unfortunately, this note must come to an end at some point, so despite the fact that there are many, many interesting things to discuss in ring theory that rely only on first principles, we must leave some of those for the future. But we saved the best topic for last.

We say that a ring R is **Noetherian** if any of the following conditions holds.

(i.) Every ascending chain of ideals of R terminates. Explicitly, for any ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$ of R, there exists an integer $N \geq 1$ sufficiently large so that $I_m = I_n$ for all integers $m, n \geq N$. (If R is not commutative, then this must hold for left- and right-ideals.)

(ii.) Every nonempty collection of ideals of R has a maximal (with respect to inclusion) element.

(iii.) Every proper ideal of R is finitely generated (cf. Proposition 7).

Proposition 24. The three conditions above are equivalent.

For the sake of brevity, we do not include a proof of Proposition 24; however, the interested reader should endeavor to prove it. One can readily show that (i.) and (ii.) are equivalent by chasing the definitions; then, it is advisable to prove that (iii.) implies (i.) and $\neg$(iii.) implies $\neg$(i.).

Even though the brilliant mathematician Emmy Noether discovered the Noetherian property of rings in the early 20th century, much of contemporary commutative algebra is undertaken in the context of Noetherian rings (and modules). One will work almost exclusively in this setting if one chooses to study commutative algebra at the University of Kansas. Gradually, we shall see and understand the importance of the Noetherian property, but for now, we show that the collection of finitely generated ideals of a ring form an Oka family (hence it suffices to establish that all of the prime ideals of a ring are finitely generated in order to conclude that a ring is Noetherian).

Proposition 25. Let R be a commutative ring. Every maximal (with respect to inclusion) element of $\{I \subseteq R \,|\, I \text{ is an ideal, and } I \text{ is not finitely generated}\}$ is prime.

Proof. We will establish that $\mathfrak{F} = \{I \subseteq R \,|\, I \text{ is a finitely generated ideal}\}$ is an Oka family. By Proposition 23, therefore, any ideal that is maximal (with respect to inclusion) with respect to the property that it is not in $\mathfrak{F}$ is prime. Put another way, every maximal (with respect to inclusion) element of $\{I \subseteq R \,|\, I \text{ is an ideal, and } I \text{ is not finitely generated}\}$ is prime, as desired.

Of course, we have that $R = 1_R R$ is a principal ideal, hence R is finitely generated so that R is in $\mathfrak{F}$. Consider an ideal I of R and any element a of R such that $I + aR$ is in $\mathfrak{F}$ and $(I :_R aR)$ is in $\mathfrak{F}$. We claim that I is in $\mathfrak{F}$. By hypothesis, there exist elements $x_1, \ldots, x_m, y_1, \ldots, y_n$ of R such that $I + aR = (x_1, \ldots, x_m)$ and $(I :_R aR) = (y_1, \ldots, y_n)$. Each of the generators of $I + aR$ is itself an element of $I + aR$, hence we have that $x_i = z_i + e_i a$ for some elements $e_i \in R$ and $z_i \in I$. Likewise, each of the generators of $(I :_R aR)$ is in $(I :_R aR)$, hence we have that $y_j a$ is in I. We claim that $I = (z_1, \ldots, z_m, y_1 a, \ldots, y_n a)$. Given an element $i \in I$, we have that $i = i + 0_R a$ is in $I + aR$ so that $i = \sum_i r_i x_i = \sum_i r_i(z_i + e_i a) = \sum_i r_i z_i + a(\sum_i e_i r_i)$. Rearranging this identity, we find that $i - \sum_i r_i z_i = a(\sum_i e_i r_i)$ so that $\sum_i e_i r_i$ is in $(I :_R aR)$. We have therefore that $\sum_i e_i r_i = \sum_j s_j y_j$ so that $i = \sum_i r_i z_i + a(\sum_j s_j y_j) = \sum_i r_i z_i + \sum_j s_j (y_j a)$ and $I \subseteq (z_1, \ldots, z_m, y_1 a, \ldots, y_n a)$. Conversely, each of the elements $z_1, \ldots, z_m, y_1 a, \ldots, y_n a$ is in I so that any R-linear combination of them is in I by hypothesis that I is an ideal of R. We conclude that $I = (z_1, \ldots, z_m, y_1 a, \ldots, y_n a)$. □

Corollary 9. Let R be a commutative ring. If every prime ideal of R is finitely generated, then every ideal of R is finitely generated. Consequently, if every prime ideal of R is finitely generated, then R is a Noetherian ring.

Proof. We leave the proof as an exercise to the reader. (Mimic the proof of Corollary 8.) □