NOETHERIAN RINGS

KEITH CONRAD

1. Introduction

In a PID, every ideal has a single generator. In a ring that is not a PID, there may not be a bound on the number of generators of all the ideals. For example, in the polynomial ring $\mathbf{Q}[X, Y]$, the ideal (X, Y) has a generating set of size 2 but not one of size 1 (it is not principal), and the ideal $(X^n, X^{n-1}Y, \ldots, XY^{n-1}, Y^n)$ in $\mathbf{Q}[X, Y]$ has a generating set of size $n + 1$ but not one of size n. Despite these variations, there is an important finiteness property of the ring $\mathbf{Q}[X, Y]$: all of its ideals are finitely generated.

Definition 1.1. A commutative ring R is called *Noetherian* if each ideal in R is finitely generated.

This name honors Emmy Noether, who in her landmark paper [6] in 1921 proved properties of such rings by conceptual methods instead of by laborious computations. She referred to such rings as those satisfying "the finiteness condition" (die Endlichkeitsbedingung). The label "Noetherian ring" is due to Chevalley [1] in 1943.

2. Examples

A simple (and boring) example of a Noetherian ring is a field. A more general class of examples is PIDs, since all of their ideals are singly generated. Noetherian rings can be regarded as a good generalization of PIDs: the property of all ideals being singly generated is often not preserved under common ring-theoretic constructions (*e.g.*, $\mathbf{Z}$ is a PID but $\mathbf{Z}[X]$ is not), but the property of all ideals being finitely generated does remain valid under many constructions of new rings from old rings. For example, we will see below that every quadratic ring $\mathbf{Z}[\sqrt{d}]$ is Noetherian; many of these rings are not PIDs.

The standard example of a non-Noetherian ring is a polynomial ring $K[X_1, X_2, \ldots]$ in infinitely many variables over a field K. Non-Noetherian rings need not be "really huge"; there is a non-Noetherian ring contained in $\mathbf{Q}[X]$: the ring of integral-valued polynomials

$$\mathrm{Int}(\mathbf{Z}) = \{f \in \mathbf{Q}[X] : f(\mathbf{Z}) \subset \mathbf{Z}\}$$

is not Noetherian.[1] This ring is bigger than $\mathbf{Z}[X]$, *e.g.*, $\binom{X}{2} = \frac{X(X-1)}{2}$ is in $\mathrm{Int}(\mathbf{Z})$ but not in $\mathbf{Z}[X]$, as is $\binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n!}$ for all $n \geq 2$.

3. Properties of Noetherian rings

Theorem 3.1. *The following conditions on a commutative ring R are equivalent:*

1. *R is Noetherian: all ideals of R are finitely generated.*
2. *each infinite increasing sequence of ideals $I_1 \subset I_2 \subset I_3 \subset \cdots$ in R eventually stabilizes: $I_k = I_{k+1}$ for all large k.*[2]

[1] See https://math.stackexchange.com/questions/408219 for a proof.

[2] The notation $\subset$ only means containment, not strict containment.

(3) *Every nonempty collection S of ideals of R contains a maximal element with respect to inclusion: there's an ideal in S not strictly contained in another ideal in S.*

The first theorem in Noether's paper [6, p. 30] is that (1) ⇒ (2), and she called this the "theorem of the finite chain" (Satz von der endlichen Kette). The standard label for property (2) is the *ascending chain condition* or ACC. Immediately after proving (1) ⇒ (2), she observed that (2) ⇒ (1) and therefore that (2) could be used as a definition of her "finiteness condition" in place of (1).

Proof. (1) ⇒ (2): If $I_1 \subset I_2 \subset \cdots$ is an increasing sequence of ideals, let $I = \bigcup_{n \geq 1} I_n$. This is an ideal since each pair of elements in I lies in a common I_n, by the increasing condition, so I is closed under addition and multiplication by elements of R. By (1), I is finitely generated. Using the increasing condition again, each finite subset of I lies in a common I_n, so a finite generating set of I is in some I_m. Thus $I \subset I_m$, and of course also $I_m \subset I$, so $I = I_m$. Then for all $n \geq m$, $I_m \subset I_n \subset I = I_m$, so $I_n = I_m$.

(2) ⇒ (1): We prove the contrapositive. Suppose (1) is false, so R has an ideal I that is not finitely generated. Pick $r_1 \in I$. Since I is not finitely generated, $I \neq (r_1)$, so there is an $r_2 \in I - (r_1)$. Since $I \neq (r_1, r_2)$, there is an $r_3 \in I - (r_1, r_2)$. Proceed in a similar way to pick r_n in I for all $n \geq 1$ by making $r_n \in I - (r_1, \ldots, r_{n-1})$ for $n \geq 2$. Then we have an increasing sequence of ideals $(r_1) \subset (r_1, r_2) \subset \cdots \subset (r_1, \ldots, r_n) \subset \cdots$ in R where each ideal is *strictly* contained in the next one, so (2) is false.

(2) ⇒ (3): We will prove the contrapositive. If (3) is false then there is a nonempty collection S of ideals in R containing no maximal member with respect to inclusion. Therefore if we start with an ideal I_1 in R, we can recursively find ideals $I_2, I_3, \ldots$ such that I_n strictly contains I_{n-1} for all $n \geq 2$. (If there were no ideal in S strictly containing I_{n-1}, then I_{n-1} would be a maximal element of S, which doesn't exist.)

(3) ⇒ (1): Let I be an ideal in R. To prove I is finitely generated, let S be the set of all finitely generated ideals contained in I. By (3), there is an $\widetilde{I} \in S$ that's contained in no other element of S, so $\widetilde{I}$ is a finitely generated ideal in I and no other finitely generated ideal of R contains $\widetilde{I}$. We will show $\widetilde{I} = I$ by contradiction, which would prove I is finitely generated. If $\widetilde{I} \neq I$, pick $a \in I - \widetilde{I}$. Since $\widetilde{I}$ is finitely generated, also $\widetilde{I} + Ra$ is finitely generated, so $\widetilde{I} + Ra \in S$. However, $\widetilde{I} + Ra$ strictly contains $\widetilde{I}$, which contradicts maximality of $\widetilde{I}$ as a member of S. Thus $\widetilde{I} = I$. □

The third condition of Theorem 3.1 shows a Noetherian ring R other than the zero ring has a maximal ideal (let S be the set of proper ideals in R) and every proper ideal I in a Noetherian ring R is contained in a maximal ideal (let S be the set of proper ideals of R that contain I). This does not need Zorn's lemma, which is used to show maximal ideals exist in *arbitrary* nonzero commutative rings. Many theorems about general commutative rings that are proved with Zorn's lemma can be proved without Zorn's lemma when the ring is Noetherian.

The following two theorems put the second condition of Theorem 3.1 to use.

Theorem 3.2. *Let R be a Noetherian ring. Each surjective ring homomorphism $R \to R$ is injective, and thus is an isomorphism.*

Proof. Let $\varphi\colon R \to R$ be a surjective ring homomorphism. For the nth iterate φ^n (the n-fold composition of φ with itself), let $K_n = \ker(\varphi^n)$. This is an ideal in R and these ideals form an increasing chain:

$$K_1 \subset K_2 \subset K_3 \subset \cdots$$

since $r \in K_n \Rightarrow \varphi^n(r) = 0 \Rightarrow \varphi^{n+1}(r) = \varphi(\varphi^n(r)) = \varphi(0) = 0$, so $r \in K_{n+1}$. Since R is a Noetherian ring, $K_n = K_{n+1}$ for some n. Pick $r \in \ker \varphi$, so $\varphi(r) = 0$. The map φ^n is surjective since φ is surjective, so $r = \varphi^n(r')$ for some $r' \in R$. Thus $0 = \varphi(r) = \varphi(\varphi^n(r')) = \varphi^{n+1}(r')$. Therefore $r' \in \ker(\varphi^{n+1}) = \ker(\varphi^n)$, so $r = \varphi^n(r') = 0$. That shows $\ker \varphi = \{0\}$, so φ is injective. □

The ring $R = K[X_1, X_2, \ldots]$ for a field K is not Noetherian and a surjective ring homomorphism $R \to R$ that is *not* injective is the shift-substitution $f(X_1, X_2, \ldots) \mapsto f(X_2, X_3, \ldots)$ for all $f \in R$.

There is no analogue of Theorem 3.2 for injective ring homomorphisms. For example, $\mathbf{R}[X]$ is a Noetherian ring since it's a PID and the substitution homomorphism $f(X) \mapsto f(X^2)$ on $\mathbf{R}[X]$ is an injective ring homomorphism that is not surjective.

Theorem 3.3. *If R is a Noetherian integral domain that is not a field, then every nonzero nonunit in R can be factored into irreducibles.*

We assume R is not a field because irreducible factorizations don't have a meaning for units, so we want R to contain some nonzero elements that aren't units.

Proof. This will be a proof by contradiction.

Suppose there is an element a in R that is not 0 or a unit and has no irreducible factorization. We will find another nonzero nonunit $b \in R$ that does not admit a factorization into irreducibles and such that there is a strict inclusion of ideals $(a) \subset (b)$.

Since a is not irreducible and it is not 0 or a unit, there is a factorization $a = bc$ where b and c are nonunits (and obviously they are not 0 either). If both b and c have an irreducible factorization, then so does a (just multiply together irreducible factorizations for b and c), so at least one of b or c has no irreducible factorization. Without loss of generality, say b has no irreducible factorization. Then since c is not a unit, the inclusion $(a) \subset (b)$ is strict.

Rewriting a as a_1 and b as a_2, we have a strict containment of ideals

$$(a_1) \subset (a_2)$$

where a_2 is a nonzero nonunit with no irreducible factorization. Using a_2 in the role of a_1 in the previous paragraph, there is a strict inclusion of ideals

$$(a_2) \subset (a_3)$$

for some nonzero nonunit a_3 that has no irreducible factorization. This argument can be repeated and leads to an infinite increasing chain of (principal) ideals

$$(a_1) \subset (a_2) \subset (a_3) \subset \cdots \tag{3.1}$$

where all inclusions are strict. This is impossible in a Noetherian ring, so we have a contradiction. Therefore nonzero nonunits without an irreducible factorization do not exist in R: all nonzero nonunits in R have an irreducible factorization. □

Theorem 3.3 is *not* saying a Noetherian integral domain has unique factorization: just because an element has an irreducible factorization doesn't mean it is unique (up to the order of multiplication and multiplication of terms by units). Many Noetherian integral domains do not have unique factorization.

Remark 3.4. If an integral domain R contains a nonzero nonunit a that has no irreducible factorization, then Theorem 3.3 tells us R can't be Noetherian, so R must contain an ideal that isn't finitely generated. In fact, the proof of Theorem 3.3 gives us an (abstract) example of an ideal in R that isn't finitely generated: the union of ideals $I := \bigcup_{n\geq 0}(a_n)$ is an ideal because $(a_n) \subset (a_{n+1})$ for all n, and I isn't finitely generated because if it were finitely generated then the containments $(a_n) \subset (a_{n+1})$ could not be strict for all n.

We now show that some basic operations on rings preserve the property of being Noetherian.

Theorem 3.5. *If R is a Noetherian ring, then so is R/I for each ideal I in R.*

Proof. Every ideal in R/I has the form J/I for an ideal J of R such that $I \subset J \subset R$. Since R is a Noetherian ring, J is a finitely generated ideal in R, and that finite generating set for J reduces to a generating set for J/I as an ideal of R/I. □

To create more examples of Noetherian rings we can use the following very important theorem.

Theorem 3.6 (Hilbert Basis Theorem)**.** *If R is a Noetherian ring, then so is $R[X]$.*

The reason for the name "Basis Theorem" is that a generating set for an ideal may be called a "basis" even if it's not linearly independent (*cf.* the modern term "Gröbner basis"). The theorem says if each ideal in R has a "finite basis", then this is true of ideals in $R[X]$.

Proof. The theorem is clear if $R = 0$, so assume $R \neq \{0\}$. To prove each ideal I in $R[X]$ is finitely generated, we assume I is not finitely generated and will get a contradiction.

We have $I \neq (0)$. Define a sequence of polynomials $f_1, f_2, \ldots$ in I as follows.

1. Pick f_1 to be an element of $I - (0)$ with minimal degree. (It is not unique.)
2. Since $I \neq (f_1)$, as I is not finitely generated, pick f_2 in $I - (f_1)$ with minimal degree. Note $\deg f_1 \leq \deg f_2$ by the minimality condition on $\deg f_1$.
3. For $k \geq 2$, if we have defined $f_1, \ldots, f_k$ in I then $I \neq (f_1, \ldots, f_k)$ since I is not finitely generated, so we may pick f_{k+1} in $I - (f_1, \ldots, f_k)$ with minimal degree.

We have $\deg f_k \leq \deg f_{k+1}$ for all k: the case $k = 1$ was checked before, and for $k \geq 2$, f_k and f_{k+1} are in $I - (f_1, \ldots, f_{k-1})$ so $\deg f_k \leq \deg f_{k+1}$ by the minimality condition on $\deg f_k$.

For $k \geq 1$, let $d_k = \deg f_k$ and c_k be the leading coefficient of f_k, so $d_k \leq d_{k+1}$ and $f_k(X) = c_k X^{d_k} +$ lower-degree terms.

The ideal $(c_1, c_2, \ldots)$ in R (an ideal of leading coefficients) is finitely generated since R is Noetherian. Each element in this ideal is an R-linear combination of finitely many c_k, so $(c_1, c_2, \ldots) = (c_1, \ldots, c_m)$ for some m.

Since $c_{m+1} \in (c_1, c_2, \ldots, c_m)$, we have

$$c_{m+1} = \sum_{k=1}^{m} r_k c_k \tag{3.2}$$

for some $r_k \in R$. From the inequalities $d_k \leq d_{m+1}$ for $k \leq m$, the leading term in $f_k(X) = c_k X^{d_k} + \cdots$ can be moved into degree d_{m+1} by using $f_k(X)X^{d_{m+1}-d_k} = c_k X^{d_{m+1}} + \cdots$, and this is in I since $f_k(X) \in I$ and I is an ideal in $R[X]$. By (3.2), the R-linear combination

$$\sum_{k=1}^{m} r_k f_k(X) X^{d_{m+1}-d_k}$$

is in the ideal $(f_1, \dots, f_m)$ and its coefficient of $X^{d_{m+1}}$ is $\sum_{k=1}^m r_k c_k$, which equals the leading coefficient c_{m+1} of $f_{m+1}(X)$ in degree d_{m+1}. The difference

$$f_{m+1}(X) - \sum_{k=1}^{m} r_k f_k(X) X^{\deg f_{m+1} - \deg f_k} \tag{3.3}$$

is in I, it is *not* 0 since $f_{m+1} \in I - (f_1, \dots, f_m)$, and it has degree *less than* d_{m+1} since the terms $c_{m+1}X^{d_{m+1}}$ cancel out. But $f_{m+1}(X)$ has minimal degree among polynomials in $I - (f_1, \dots, f_m)$, and (3.3) is in $I - (f_1, \dots, f_m)$ with lower degree than d_{m+1}. That's a contradiction. Thus I is finitely generated. □

To summarize this proof in a single phrase, "use an ideal of leading coefficients".

In the proof, the Noetherian property of R is used where we said $(c_1, c_2, \dots) = (c_1, \dots, c_m)$ for some m. All we need to get the contradiction in the proof is $c_{m+1} \in (c_1, \dots, c_m)$ for some m. Since $(c_1) \subset (c_1, c_2) \subset (c_1, c_2, c_3) \subset \cdots$, what we need is the following property: for each infinite increasing sequence of ideals $I_1 \subset I_2 \subset I_3 \subset \cdots$ in R, $I_m = I_{m+1}$ for some m. Of course this is implied by the Noetherian property, but it also implies the Noetherian property since a non-Noetherian ring has an infinite increasing sequence of ideals with strict containments at each step: see the proof of (2) ⇒ (1) in Theorem 3.1.

Remark 3.7. Our proof of the Hilbert Basis Theorem, which is due to Sarges [7], is by contradiction and thus is not constructive. A constructive proof runs as follows. For $R \neq 0$, I a nonzero ideal in $R[X]$, and $n \geq 0$, let L_n be the set of leading coefficients of polynomials in I of degree *at most* n together with 0. This is an ideal in R by the way polynomials add and get scaled by R. (While L_n might be (0) for small n, $L_n \neq (0)$ for large n since I contains a nonzero polynomial and multiplying that by powers of X gives us polynomials in I of all higher degrees.) Since $L_n \subset L_{n+1}$, the ideals $\{L_n\}$ in R stabilize at some point, say $L_n = L_m$ for $n \geq m$. (Thus L_m is generated by the leading coefficients of *all* nonzero polynomials in I, so we could have defined L_m that way.) Each L_n has finitely many generators. When $L_n \neq (0)$, let P_n be a finite set of polynomials of degree at most n in I whose leading coefficients generate L_n. The union of the finite sets P_n for $n \leq m$ where $L_n \neq (0)$ is a generating set for I [4, Sect. 7.10]. This way of proving Hilbert's basis theorem is essentially due to Artin, according to van der Waerden [8].

Where in the proof of Theorem 3.6 did we use the assumption that R is Noetherian? It is how we know the ideals $(c_1, \dots, c_k)$ for $k \geq 1$ stabilize for large k, so $c_{m+1} \in (c_1, \dots, c_m)$ for some m. The contradiction we obtain from that really shows $c_{m+1} \notin (c_1, \dots, c_m)$ for all m, so the proof of Theorem 3.6 could be viewed as proving the contrapositive: if $R[X]$ is not Noetherian then R is not Noetherian.

The converse of Theorem 3.6 is true: if the ring $R[X]$ is Noetherian, then so is the ring R by Theorem 3.5, since $R \cong R[X]/(X)$

Corollary 3.8. *If R is a Noetherian ring, then so is $R[X_1, \dots, X_n]$ for all $n \geq 1$.*

Proof. We induct on n. The case $n = 1$ is Theorem 3.6. For $n \geq 2$, write $R[X_1, \dots, X_n]$ as $R[X_1, \dots, X_{n-1}][X_n]$, with $R[X_1, \dots, X_{n-1}]$ being Noetherian by the inductive hypothesis, so we are reduced to the base case. □

Remark 3.9. Corollary 3.8 in the special cases $R = \mathbf{C}$ and $R = \mathbf{Z}$ were proved by Hilbert in 1890 [3, Theorem I, p. 474], [3, Theorem II, p. 485] as a pure existence theorem, not by an algorithm.[3] This is what first made Hilbert famous in mathematics. Earlier, Gordan [2] settled the case $n = 2$ of Corollary 3.8 for $R = \mathbf{C}$ in 1868 by long calculations and spent 20 years unsuccessfully working on $n = 3$. Hilbert's proof that $\mathbf{C}[X_1, \ldots, X_n]$ is Noetherian for all n was revolutionary, illustrating the power of existence proofs over constructive methods, and this became characteristic of much of modern mathematics. With the rise of fast computers in the late 20th century, generating sets for polynomial ideals can be computed routinely with Gröbner bases, which are a multivariable polynomial replacement for the Euclidean algorithm of polynomials in one variable.

Using polynomial rings and quotient rings, we now can build lots of Noetherian rings.

Example 3.10. The quadratic ring $\mathbf{Z}[\sqrt{d}]$ for a nonsquare integer d is Noetherian. That follows from viewing $\mathbf{Z}[\sqrt{d}]$ as $\mathbf{Z}[X]/(X^2 - d)$: evaluation at $\sqrt{d}$ is a surjective ring homomorphism $\mathbf{Z}[X] \to \mathbf{Z}[\sqrt{d}]$ with kernel $(X^2 - d)$,[4] so $\mathbf{Z}[\sqrt{d}] \cong \mathbf{Z}[X]/(X^2 - d)$. The ring $\mathbf{Z}[X]$ is Noetherian by Hilbert's basis theorem, and $\mathbf{Z}[X]/(X^2 - d)$ is Noetherian by Theorem 3.5, so $\mathbf{Z}[\sqrt{d}]$ is Noetherian.

Example 3.11. The rings $\mathbf{Z}[\sqrt{2}, \sqrt{3}]$ and $\mathbf{Z}[i, \sqrt[3]{2}, \sqrt[7]{10}]$ are Noetherian since $\mathbf{Z}[\sqrt{2}, \sqrt{3}] \cong \mathbf{Z}[X, Y]/(X^2 - 2, Y^2 - 3)$ and $\mathbf{Z}[i, \sqrt[3]{2}, \sqrt[7]{10}] \cong \mathbf{Z}[X, Y, Z]/(X^2 + 1, Y^3 - 2, Z^7 - 10)$.

Example 3.12. The ring $\mathbf{Z}[X, 1/X]$ is Noetherian by viewing it as $\mathbf{Z}[X, Y]/(XY - 1)$.

Example 3.13. For a field K and ideal I in $K[X_1, \ldots, X_n]$, the ring $K[X_1, \ldots, X_n]/I$ is Noetherian since K is trivially Noetherian. For instance, $\mathbf{R}[X, Y, Z]/(X^2 + Y^3 - Z^5, XYZ)$ is Noetherian.

Remark 3.14. Besides polynomials in finitely many variables, formal power series in finitely many variables are important. For a Noetherian ring R, the formal power series ring $R[[X_1, \ldots, X_n]]$ is Noetherian (first proved by Chevalley [1, Lemma 8]). The proof of this reduces to the case $n = 1$ by induction, as in the polynomial case, since $R[[X_1, \ldots, X_n]]$ is $R[[X_1, \ldots, X_{n-1}]][[X_n]]$ when $n \geq 2$. Formal power series need not have a leading coefficient, so the proof in the polynomial case doesn't work directly for power series. What can be used with power series instead of a leading term is a lowest degree term, so the proof of Theorem 3.5 can be adapted to formal power series by changing highest-degree coefficients into lowest-degree coefficients. An infinite "limiting process" occurs in the proof since the multipliers on a generating set for the ideal are power series. See [4, Theorem 7.11].

The last property we'll discuss about Noetherian rings is their "primary ideal decomposition," which is an analogue in all Noetherian rings of prime-power factorization in $\mathbf{Z}$. Each $n > 1$ can be written as a product of prime powers: $n = p_1^{e_1} \cdots p_k^{e_k}$ for primes p_i and $e_i \geq 1$. Viewing this as an equation of principal ideals,

$$(n) = (p_1^{e_1} \cdots p_k^{e_k}) = (p_1^{e_1}) \cap \cdots \cap (p_k^{e_k}).$$

We'll show each proper ideal in a Noetherian ring is a finite intersection of primary ideals, which are a generalization of the ideals (p^e) in $\mathbf{Z}$.

[3] Hilbert could not use the proof that we gave for his basis theorem, since he didn't have the concept of a Noetherian ring in full generality available to him.

[4] Although $\mathbf{Z}[X]$ is not Euclidean, there is unique division with remainder by a *monic* polynomial, such as $X^2 - d$. If $f(\sqrt{d}) = 0$ where $f(X) \in \mathbf{Z}[X]$ and we write $f(X) = (X^2 - d)Q(X) + R(X)$ where $R(X) = a + bX$, then the condition $f(\sqrt{d}) = 0$ implies $a + b\sqrt{d} = 0$, so $a = b = 0$ and thus $R(X) = 0$, so $f(X) \in (X^2 - d)$.

Definition 3.15. Say an ideal Q in a commutative ring R is *primary* if $Q \neq R$ and the zero divisors in R/Q are nilpotent: if $ab \equiv 0 \bmod Q$ and $a \not\equiv 0 \bmod Q$, then $b^n \equiv 0 \bmod Q$ for some $n \geq 1$. Equivalently, if $ab \equiv 0 \bmod Q$ then $a \equiv 0 \bmod Q$ or $b^n \equiv 0 \bmod Q$ for some n.

Example 3.16. For a prime ideal P in R, the only zero divisor in R/P is $\overline{0}$, so a prime ideal is a primary ideal.

Example 3.17. For $R = \mathbf{Z}$, its primary ideals are (0) and (p^e) for prime numbers p and $e \geq 1$, so we can think of primary ideals as a generalization of prime powers.[5]

To realize ideals as intersections of primary ideals, it's useful to have the following names for ideals that are or are not intersections of other ideals.

Definition 3.18. In a commutative ring R, an ideal I is called *reducible* if $I = J \cap J'$ for ideals J and J' strictly containing I. An *irreducible* ideal is proper and not reducible.

Irreducibility of I means $I \neq R$ and whenever $I = J \cap J'$ for ideals J and J' in R, either J or J' is I.

Example 3.19. For $R = \mathbf{Z}$, intersections of ideals are related to least common multiples: $(a) \cap (b) = (\operatorname{lcm}(a, b))$. For example, $(6) \cap (9) = (18)$. If $(a) \cap (b) = (81)$ then $\operatorname{lcm}(a, b) = 81$, and the only way that can happen is if $a = \pm 81$ or $b = \pm 81$ (why?), so $(a) = (81)$ or $(b) = (81)$. More generally, if $(a) \cap (b) = (p^e)$ for a prime number p and $e \geq 1$, then $(a) = (p^e)$ or $(b) = (p^e)$, so (p^e) is an irreducible ideal in $\mathbf{Z}$. The irreducible ideals in $\mathbf{Z}$ are (0) and prime-power ideals (p^e).

Theorem 3.20. *In a nonzero Noetherian ring, each proper ideal is an intersection of finitely many irreducible ideals.*

Proof. Let S be the set of proper ideals that are *not* an intersection of finitely many irreducible ideals. To show $S = \emptyset$, assume $S \neq \emptyset$. Since our ring is Noetherian, S contains a maximal element by Theorem 3.1(3), say I. Then I is a proper ideal and I is not irreducible by the definition of S, so $I = J \cap J'$ for two ideals J and J' that strictly contain I. The ideals J and J' are proper, *e.g.*, if $J = (1)$ then $I = (1) \cap J' = J'$, but $J' \neq I$.

Since I is a strict subset of J and J', which are both proper, the maximality of I in S implies J and J' are each an intersection of finitely many irreducible ideals:

$$J = I_1 \cap \cdots \cap I_k, \qquad J' = I'_1 \cap \cdots \cap I'_\ell,$$

where I_i and I'_j are irreducible. Then

$$I = J \cap J' = I_1 \cap \cdots \cap I_k \cap I'_1 \cap \cdots \cap I'_\ell,$$

which contradicts the condition $I \in S$. Thus $S = \emptyset$. □

Lemma 3.21. *Let I be an ideal in a commutative ring R.*

(a) *I is irreducible in R if and only if the zero ideal $(\overline{0})$ in R/I is irreducible.*
(b) *I is primary in R if and only if the zero ideal $(\overline{0})$ in R/I is primary.*

Property (b) is analogous to saying an ideal P in R is a prime ideal if and only if the zero ideal in R/P is a prime ideal.

[5] A power of a prime ideal need not be primary, but powers of maximal ideals are: see https://math.stackexchange.com/questions/93478. Also, a primary ideal need not be a power of a prime ideal despite that being the motivation behind primary ideals: see https://math.stackexchange.com/questions/93415.

Proof. (a) First suppose I is irreducible in R, so $I \neq R$. Then $R/I \neq \{\overline{0}\}$, so $(\overline{0})$ is a proper ideal of R/I.

Each ideal in R/I has a unique description as J/I for an ideal J in R that contains I. To prove $(\overline{0})$ is irreducible in R/I, suppose $(\overline{0})$ is an intersection of two ideals in R/I: $(\overline{0}) = J/I \cap J'/I$ where J and J' are ideals in R containing I. Then $(\overline{0}) = (J \cap J')/I$, so $I = J \cap J'$. Irreducibility of I in R implies $J = I$ or $J' = I$, so J/I or J'/I is $(\overline{0})$.

The converse direction of (a) is left to the reader.

(b) Saying I is primary in R means $I \neq R$ and zero divisors in R/I are nilpotent. Saying $(\overline{0})$ is primary in R/I means $(\overline{0}) \neq R/I$ and zero divisors in $(R/I)/(\overline{0})$ are nilpotent. The conditions "$I \neq R$" and "$(\overline{0}) \neq R/I$" are equivalent and $(R/I)/(\overline{0}) \cong R/I$, so the properties of I being primary in R and $(\overline{0})$ being primary in R/I are equivalent. □

Theorem 3.22. *In a nonzero Noetherian ring every irreducible ideal is a primary ideal.*

Proof. By Theorem 3.5 and Lemma 3.21, it suffices to show that in a Noetherian ring, if the zero ideal is irreducible then it is primary.

Suppose (0) is an irreducible ideal in a Noetherian ring R and $xy = 0$ in R. We want to prove $x = 0$ or y is nilpotent.

To each $r \in R$ is an associated ideal called its annihilator: $\text{Ann}(r) = \{a \in R : ar = 0\}$. Consider the following increasing chain of ideals in R using powers of y:

$$\text{Ann}(y) \subset \text{Ann}(y^2) \subset \text{Ann}(y^3) \subset \cdots .$$

Since R is Noetherian, this chain stabilizes: for some $n \geq 1$, $\text{Ann}(y^m) = \text{Ann}(y^n)$ for all $m \geq n$. We're going to use $\text{Ann}(y^{n+1}) = \text{Ann}(y^n)$ to prove $x = 0$ or $y^n = 0$.

Claim: $(x) \cap (y^n) = (0)$.

Pick $a \in (x) \cap (y^n)$. Since $a \in (x)$ and $xy = 0$, we have $ay = 0$. Since $a \in (y^n)$ we have $a = by^n$, so $0 = ay = by^{n+1}$, so $b \in \text{Ann}(y^{n+1}) = \text{Ann}(y^n)$. Thus $by^n = 0$, so $a = 0$. That proves the claim.

From the claim and irreducibility of (0) in R, $(x) = (0)$ or $(y^n) = (0)$. Therefore $x = 0$ or $y^n = 0$, so (0) is a primary ideal in R. □

Theorem 3.23. *In a nonzero Noetherian ring, each proper ideal is an intersection of finitely many primary ideals.*

Proof. This follows from Theorems 3.20 and 3.22. □

Remark 3.24. The proof of Theorem 3.23, if you unravel it, has three steps: (i) define irreducible ideals, (ii) show proper ideals are finite intersections of irreducible ideals and (iii) show irreducible ideals are primary. There is a similar approach to proving each nonzero finite abelian group A is a direct sum of cyclic subgroups of prime power order: define indecomposable finite abelian groups as nonzero and not a direct sum of nonzero subgroups, show each nonzero A is a direct sum of indecomposable subgroups, and show indecomposable finite abelian groups are cyclic of prime-power order.[6]

Theorem 3.23 was first proved for the polynomial ring $\mathbf{C}[X_1, \ldots, X_n]$ by Lasker [5] in 1905. Noether's much shorter proof, valid for all Noetherian rings, was a powerful illustration of her abstract approach to studying rings and ideals, which proved results in a general setting that previously seemed intimately tied to computations with polynomials.

The primary ideal decomposition in Noetherian rings can be refined to include uniqueness aspects. This is treated in books on commutative algebra.

[6] See https://kconrad.math.uconn.edu/blurbs/grouptheory/finite-abelian.pdf.

References

[1] C. Chevalley, *On the Theory of Local Rings*, Ann. of Math. **44** (1943), 690–708. URL https://www.jstor.org/stable/1969105.

[2] P. Gordan, *Beweis, dass jede Covariante und Invariante einer binären Form eine ganze Function mit numerischen Coefficienten einer endlichen Anzahl solcher Formen ist*, J. Reine Angew. Mathematik **69** (1868), 323–354. URL https://eudml.org/doc/148066.

[3] D. Hilbert, *Ueber die Theorie der algebraischen Formen*, Math. Annalen **36** (1890), 473–534. URL https:// eudml.org/doc/157506.

[4] N. Jacobson, "Basic Algebra II", 2nd ed., W. H. Freeman & Co., New York, 1989.

[5] E. Lasker, *Zur Theorie der Moduln und Ideale*, Math. Annalen **60** (1905), 20–116, URL https://eudml.org/doc/158174.

[6] E. Noether, *Idealtheorie in Ringbereichen*, Math. Annalen **83** (1921), 24–66. URL https://eudml.org/doc/158855. English translation by D. Berlyne https://arxiv.org/abs/1401.2577.

[7] H. Sarges, *Ein Beweis des Hilbertschen Basissatzes*, J. Reine Angew. Math. **283** (1976), 436–437. URL https://eudml.org/doc/151744.

[8] B. L. van der Waerden, *On the sources of my book Moderne Algebra*, Historia. Math. **2** (1975), 31–40. URL https://core.ac.uk/download/pdf/82253306.pdf.