Miscellaneous results on prime ideals

Rodney Coleman, Laurent Zwald

Miscellaneous results on prime ideals

Rodney Coleman, Laurent Zwald

December 4, 2020

Abstract

In these notes, we present various useful results concerning prime ideals. We characterize prime and maximal ideals in $\mathbf{Z}[X]$ and introduce the height of an ideal and the dimension of a ring. In particular, we provide bounds for the dimension of a polynomial ring. We also study in detail radicals and certain proprieties of artinian and noetherian rings. We give a proof of the prime avoidance lemma.

Prime ideals principal implies all ideals principal

A commutative ring is a principal ideal ring if every ideal can be generated by a single element. In particular, an integral domain is a principal ideal domain (PID), if every ideal can be generated by a single element. Our aim here is to show that it is sufficient to consider prime ideals.

Let R be a ring such that every prime ideal is principal and Σ the set of ideals which are not principal. We aim to show that Σ is empty. Suppose that this is not the case. We define an order on Σ by inclusion. Let $(I_t)_{t\in T}$ be a chain in Σ and $I = \cup_{t\in T} I_t$. We claim that $I \in \Sigma$. If $I \notin \Sigma$, then $I = (x)$, for some $x \in R$. There exists an index $t \in T$ such that $x \in I_t$ and so we have

$$(x) \subset I_t \subset I = (x),$$

which implies that $I_t = (x)$, a contradiction, because I_t is not principal. Hence $I \in \Sigma$. By Zorn's lemma, there exists a maximal ideal $J \in \Sigma$. We will show that J is a prime ideal, which is a contradiction, because all prime ideals are principal.

Let $a_1, a_2 \in R \setminus J$. Since J is maximal, the ideals (J, a_1) and (J, a_2) do not belong to Σ. Therefore there exist $x_1, x_2 \in R$ such that $(J, a_1) = (x_1)$ and $(J, a_2) = (x_2)$. We claim that $(x_1x_2) = (J, a_1a_2)$. First we have

$$(x_1x_2) = (x_1)(x_2) = (J, a_1)(J, a_2) \subset (J, a_1a_2).$$

Now we set

$$J_i = \{y \in R : yx_i \in J\},$$

for $i = 1, 2$. The J_i are ideals containing J. We will show that $J = J_i(x_i)$, for $i = 1, 2$. ($J_i(x_i)$ is the product of the ideals J_i and (x_i).) By definition of J_i, we have $J_i(x_i) \subset J$. On the other hand, if $x \in J$, then $x \in (J, a_i) = (x_i)$, which implies that $x = u_ix_i$, with $u_i \in R$. As $x \in J$, $u_i \in J_i$ so $x \in J_i(x_i)$. We have shown that $J = J_i(x_i)$, as required.

Our next step is to show that $J = J_i$. We have observed above that $J \subset J_i$. If the inclusion is proper, then J_i is principal and so we may write $J_i = (y_i)$, for some $y_i \in R$. Then

$J = J_i(x_i) = (y_i x_i)$, so J is a principal ideal, contradicting the fact that $J \in \Sigma$. Thus we have $J = J_1 = J_2$.

We now show that $(J, a_1a_2) = (x_1x_2)$. First we have

$$J = J_1(x_1) = J(x_1) = J_2(x_2)(x_1) = J(x_1x_2) \subset (x_1x_2).$$

Since $a_1a_2 \in (J, a_1)(J, a_2) = (x_1x_2)$, we conclude that $(J, a_1a_2) \subset (x_1x_2)$. Above we saw that $(x_1x_2) \subset (J, a_1a_2)$, so we have the desired equality.

Now we complete the argument. If $a_1a_2 \in J$, then $(J, a_1a_2) = J$ and so J is principal, a contradiction. We have shown that $a_1, a_2 \notin J$ implies that $a_1a_2 \notin J$, hence J is a prime ideal. Thus J is a prime ideal which is not principal. However, this contradicts the hypothesis that every prime ideal is principal. It follows that Σ is empty, i.e., R is a PID. We have proved:

PIDth1 **Theorem 1** *If R is a commutative ring in which every prime ideal is principal, then R is a principal ideal ring. In particular, an integral domain in which every prime ideal is principal is a principal ideal domain (PID).*

Corollary 1 *If D is a Dedekind domain which is also a UFD, then D is a PID.*

PROOF From Theorem PIDth1 it is sufficient to show that a prime ideal P in D is principal. If $P = \{0\}$, then there is nothing to prove, so let P be a nontrivial prime ideal and x a nonzero element in P. As $P \neq D$, we may write $x = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, where the p_i are irreducible elements in D and s and the α_i positive integers. Since P is a prime ideal, at least one of the p_i belongs to P. Without loss of generality, let us suppose that $p_1 \in P$. Then $(p_1) \subset P$. As D is a UFD and p_1 irreducible, hence prime, the ideal (p_1) is a prime ideal. However, prime ideals in a Dedekind domain are maximal, thus $(p_1) = P$ and it follows that P is a principal ideal. □

The prime and maximal ideals in $\mathbf{Z}[X]$

We aim to show that the prime ideals in $\mathbf{Z}[X]$ have one of the following forms:

- 1. $P = (0)$;
- 2. $P = \mathbf{Z}[X]p$, for some prime number p;
- 3. $P = \mathbf{Z}[X]\pi(X)$, for some irreducible nonconstant polynomial $\pi(X)$ in $\mathbf{Z}[X]$;
- 4. $P = \mathbf{Z}[X]p + \mathbf{Z}[X]\pi(X)$, where p is a prime number and $\pi(X)$ is a polynomial in $\mathbf{Z}[X]$ irreducible modulo p.

First we show that the above ideals are prime:

1. If $P = (0)$, then P is clearly prime.

2. Suppose that $P = \mathbf{Z}[X]p$, for some prime number p. The elements of P have the form $f(X) = \sum_{i=0}^{n} a_i X^i$, where $p|a_i$, for all i. Suppose that $k(X) = g(X)h(X) \in P$, with $g(X) = \sum_{i=0}^{r} b_i X^i$ and $h(X) = \sum_{i=0}^{s} c_i X^i$, and that both $g(X)$ and $h(X)$ do not belong to P. Then there are coefficients of g and h not divisible by p. Let b_k (resp. c_l), be the first coefficient of g (resp. h) not divisible by p. If $g(X)h(X) = k(X) = \sum_{i=0}^{r+s} d_i X^i$, then

$$d_{k+l} = b_0c_{k+l} + b_1c_{k+l-1} + \cdots + b_kc_l + \cdots + b_{k+l}c_0.$$

Now p divides all terms other than $b_k c_l$, so $p \not| d_{k+l}$, a contradiction, hence $g \in P$ or $h \in P$ and so P is prime.

3. The elements of P have the form $f(X) = \sum_{i=0}^{n} \pi(X) a_i X^i = \sum_{i=0}^{n} a_i(X) X^i$, where $\pi(X) | a_i(X)$. To show that P is prime, we may use an argument analogous to that used in 2. Suppose that $f(X) = g(X)h(X) \in P$, where both $g(X)$ and $h(X)$ do not belong to P. We may write $g(X) = \sum_{i=0}^{r} b_i(X) X^i$ and $h(X) = \sum_{i=0}^{s} c_i(X) X^i$. There are coefficients of g and h not divisible by $\pi(X)$. Let $b_k(X)$ (resp. $c_l(X)$) be the first coefficient of g (resp. h) not divisible by $\pi(X)$. If $g(X)h(X) = \sum_{i=0}^{r+s} d_i(X) X^i$, then

$$d_{k+l}(X) = b_0(X)c_{k+l}(X) + b_1(X)c_{k+l-1}(X) + \cdots + b_k(X)c_l(X) + \cdots + b_{k+l}(X)c_0(X).$$

Now $\pi(X)$ divides all terms other than $b_k(X)c_l(X)$. (If $\pi(X)$ divides the product $b_k(X)c_l(X)$, then $\pi(X)$ must divide one of the polynomials in the product, because $\pi(X)$ is irreducible, hence prime.) This implies that $\pi(X)$ does not divide $d_{k+l}(X)$, a contradiction, hence $g(X) \in P$ or $h(X) \in P$, i.e., P is a prime ideal.

4. Let α be the standard mapping taking $g \in \mathbf{Z}[X]$ to $\bar{g} \in \mathbf{F}_p[X]$ and β the standard mapping taking elements of $\mathbf{F}_p[X]$ into $\mathbf{F}_p[X]/(\bar{\pi})$. We set $\phi = \beta \circ \alpha$. The kernel of ϕ is P and so $\mathbf{Z}[X]/P \simeq \mathbf{F}_p[X]/(\bar{\pi})$, which is a field. Thus P is a maximal ideal and so prime.

We now need to show that these ideals are the only prime ideals in $\mathbf{Z}[X]$. Let P be a prime ideal in $\mathbf{Z}[X]$. For the contraction of P to $\mathbf{Z}$, i.e., the intersection of P with $\mathbf{Z}$, there are two possibilities: $P \cap \mathbf{Z} = (0)$ or $P \cap \mathbf{Z} = (p)$, for some prime number p.

Case 1 $P \cap \mathbf{Z} = (0)$

If $P = (0)$, then we are done. Suppose that this is not the case and let $S = \mathbf{Z} \setminus (0)$. Then $S \cap P = \emptyset$. As S is a multiplicative set in $\mathbf{Z}[X]$, we may localize $\mathbf{Z}[X]$ at S to obtain $\mathbf{Q}[X]$. The ideal $S^{-1}P$ is prime in $\mathbf{Q}[X]$ and so has the form $\mathbf{Q}[X]\pi(X)$, where $\pi(X)$ is irreducible in $\mathbf{Q}[X]$. We may suppose that $\pi(X)$ has integer coefficients whose *gcd* is 1, i.e., π is a primitive polynomial in $\mathbf{Z}[X]$. We claim that $P = \mathbf{Z}[X]\pi(X)$.

The elements of $S^{-1}P$ have the form $\frac{r(X)}{s}$, with $r(X) \in P$ and $s \in S$, so $\pi(X)$ has this form and we may write $s\pi(X) \in P$, for some $s \in \mathbf{Z}$; since P is a prime ideal in $\mathbf{Z}[X]$ and $s \notin P$, we must have $\pi(X) \in P$. Thus $\mathbf{Z}[X]\pi(X) \subset P$.

We now show that $P \subset \mathbf{Z}[X]\pi(X)$. If $f \in P$, then $f \in S^{-1}P$ and so we may write $f(X) = \frac{r(X)}{s}\pi(X)$, where r has integer coefficients. Writing $c(g)$ for the content of a polynomial $g(X) \in \mathbf{Z}[X]$ and noting that $c(\pi) = 1$, we have

$$\begin{aligned} sf(X) = r(X)\pi(X) &\implies sc(f) = c(r)c(\pi) = c(r) \\ &\implies s = \frac{c(r)}{c(f)} \\ &\implies f(X) = \frac{c(f)}{c(r)} r(X)\pi(X) \in \mathbf{Z}[X]\pi(X), \end{aligned}$$

because $c(r)$ divides all the coefficients of $r(X)$. Therefore $P \subset \mathbf{Z}[X]\pi(X)$ and it follows that $P = \mathbf{Z}[X]\pi(X)$.

It should be noted that $\pi(X)$ is irreducible in $\mathbf{Q}[X]$, hence in $\mathbf{Z}[X]$. We also notice that $\pi(X)$ is not a constant polynomial: since $c(\pi) = 1$, the only possibility would be that $\pi = 1$, which is not possible, because P is properly contained in $\mathbf{Z}[X]$.

Case 2 $P \cap \mathbf{Z} = (p)$

Let α be the standard mapping defined above. We claim that the image of P under α in $\mathbf{F}_p[X]$ is a prime ideal. First we notice that the kernel of α is equal to $\mathbf{Z}[X]p$, which is a subset of P.

If $1 \in \alpha(P)$, then there exists $u \in P$ such that $\alpha(u) = 1$. As $\alpha(1) = 1$, we have $1 - u \in \mathrm{Ker}\,(\alpha) \subset P$ and it follows that $1 = u + (1 - u) \in P$, which is impossible, because P is a proper subset of $\mathbf{Z}[X]$. Therefore $\alpha(P)$ is properly contained in $\mathbf{F}_p[X]$.

Suppose now that $x, y \in \mathbf{F}_p[X]$ and $xy \in \alpha(P)$. There exist $a, b \in \mathbf{Z}[X]$ such that $\alpha(a) = x$, and $\alpha(b) = y$. Then $\alpha(ab) = \alpha(a)\alpha(b) \in \alpha(P)$. Thus there exists $c \in P$ such that $\alpha(ab) = \alpha(c)$, which implies that $ab - c \in \mathrm{Ker}\,\alpha \subset P$. Hence $ab \in P$. As P is a prime ideal, either $a \in P$ or $b \in P$, therefore $x = \alpha(a) \in \alpha(P)$ or $y = \alpha(b) \in \alpha(P)$. Thus $\alpha(P)$ is a prime ideal as claimed.

The prime ideals in $\mathbf{F}_p[X]$ are (0) and the ideals of the form $\mathbf{F}_p[X]q(X)$, where $q(X)$ is a monic irreducible polynomial in $\mathbf{F}_p[X]$. If $\alpha(P) = (0)$, then $\mathbf{Z}[X]p \subset P \subset \mathrm{Ker}\,(\alpha) = \mathbf{Z}[X]p$, so $P = \mathbf{Z}[X]p$. We now consider the other possibilty.

Suppose that $\alpha(P) = \mathbf{F}_p[X]q(X)$, where $q(X)$ is a monic irreducible polynomial in $\mathbf{F}_p[X]$. There is a polynomial $\pi(X) \in \mathbf{Z}[X]$ such that $\alpha(\pi(X)) = q(X)$. Then $\pi(X)$ is irreducible modulo p.

We claim that $P = \mathbf{Z}[X]p + \mathbf{Z}[X]\pi(X)$. First, $P \cap \mathbf{Z} = (p)$ implies that $p \in P$. Clearly, $\pi(X) \in Q = \alpha^{-1}(\alpha(P))$, which is a proper ideal in $\mathbf{Z}[X]$, because $1 \notin Q$. From Corollary 2 (see below), a nonzero prime ideal in a PID is maximal; as $P \subset Q$ and P is nonzero, we have $P = Q$, hence $\pi(X) \in P$. Therefore $\mathbf{Z}[X]p + \mathbf{Z}[X]\pi(X) \subset P$. PIDcor1a

We now show that $P \subset \mathbf{Z}[X]p + \mathbf{Z}[X]\pi(X)$. Let $f(X) \in P$. There exists $\bar{g} \in \mathbf{F}_p[X]$ such that $\bar{g}(X)q(X) = \bar{f}(X)$ or $\bar{g}(X)q(X) - \bar{f}(X) = 0$. It follows that $g(X)\pi(X) - f(X) \in \mathbf{Z}[X]p$, so $f(X) \in \mathbf{Z}[X]p + \mathbf{Z}[X]\pi[X]$ and we have $P \subset \mathbf{Z}[X]p + \mathbf{Z}[X]\pi(X)$. Hence the equality $P = \mathbf{Z}[X]p + \mathbf{Z}[X]\pi(X)$.

Maximal ideals in $\mathbf{Z}[X]$

We have seen that the prime ideals of type 4. are maximal. Clearly, if $P = (0)$, then P is not maximal. If $P = \mathbf{Z}[X]p$, then P is properly contained in $\mathbf{Z}[X]p + \mathbf{Z}[X]X \neq \mathbf{Z}[X]$, and so is not maximal. Finally, we consider prime ideals of type 3. To simplify the notation, let us write $(\pi(X))$ for $\mathbf{Z}[X]\pi(X)$. We aim to show that $\mathbf{Z}[X]/(\pi(X))$ is not a field, which implies that $(\pi(X))$ is not a maximal ideal. As the polynomials $\pi(X)$, $\pi(X)+1$ and $\pi(X)-1$ have at most a finite number of roots in $\mathbf{Z}$, we can find $a \in \mathbf{Z}$ such that $\pi(a) \neq 0, \pm 1$. Let p be a prime number dividing $\pi(a)$. We consider the mapping

$$\phi : \mathbf{Z}[X]/(\pi(X)) \longrightarrow \mathbf{Z}/(p), f(X) + (\pi(X)) \longmapsto f(a) + (p),$$

where $(p) = \mathbf{Z}p$. The mapping ϕ is a well-defined ring homomorphism, which is not injective, because $\mathbf{Z}[X]/(\pi(X))$ is infinite and $\mathbf{Z}/(p)$ is finite. This implies that $\mathrm{Ker}\,(\phi) \neq (0)$. Also, ϕ is not the zero mapping, because $\phi(1 + (\pi)) = 1 + (p) \neq (p)$. It follows that $(0) \subset \mathrm{Ker}\,(\phi) \subset \mathbf{Z}[X]/(\pi(X))$, where the inclusions are strict. Since $\mathbf{Z}[X]/(\pi(X))$ contains a nontrivial ideal, it is not a field and so $(\pi(X))$ is not a maximal ideal in $\mathbf{Z}[X]$.

Heights and Dimensions

If P is a prime ideal in a commutative ring R and

$$P_0 \subset P_1 \subset \cdots \subset P_n = P$$

a chain of distinct prime ideals in P, then we call n the length of the chain. The height of P, written $\mathrm{ht}(P)$, is the supremum of lengths of chains of prime ideals included in P. The dimension of R, written $\dim(R)$, is the supremum of heights of prime ideals in R. We notice that we may also define $\dim(R)$ to be the supremum of lengths of chains of prime ideals in R. A field has dimension 0, because (0) is its unique prime ideal.

For a general ideal I we define the height as follows:

$$\mathrm{ht}(I) = \inf_{I \subset P, P \in Spec(R)} \mathrm{ht}(P).$$

There is no difficulty in seeing that, for a prime ideal P', we have

$$\inf_{P' \subset P, P \in Spec(R)} \mathrm{ht}(P) = \mathrm{ht}(P'),$$

so this definition of height for a general ideal generalizes that for a prime ideal.

We should also notice that $I \subset J$ implies that $\mathrm{ht}(I) \leq \mathrm{ht}(J)$. Moreover, if I and J are prime ideals and the inclusion is strict, then the inequality is strict.

We begin with two elementary lemmas.

Lemma 1 *If I is an ideal in a commutative ring R, then*

$$ht(I) + \dim(R/I) \leq \dim(R).$$

PROOF If $s \leq \dim(R/I)$, we may find distinct prime ideals $Q_i \in R$, with $i = 0, 1, \ldots, s$, such that

$$I \subset Q_0 \subset Q_1 \subset \cdots \subset Q_s.$$

Then $\mathrm{ht}(Q_0) \geq \mathrm{ht}(I) = r$, so we may find distinct prime ideals P_i, with $i = 0, 1, \ldots, r$, such that

$$P_0 \subset P_1 \subset \cdots \subset P_r = Q_0.$$

Moreover,

$$P_0 \subset P_1 \subset \cdots \subset P_r = Q_0 \subset Q_1 \subset \cdots \subset Q_s$$

is a chain of distinct prime ideals in R of length $r + s$. It follows that $\dim(R) \geq \mathrm{ht}(I) + s$ and so $\dim(R) - \mathrm{ht}(I)$ is an upper bound on lengths of chains of distinct prime ideals contained in R/I, which implies that $\dim(R) - \mathrm{ht}(I) \geq \dim(R/I)$; □

Lemma 2 *If (R, M) is a local ring, then*

$$\dim(R) = ht(M).$$

In particular, if P is prime ideal in a commutative ring R and R_P is the localization of R at P, then

$$\dim(R_P) = ht(P).$$

PROOF Any chain of distinct prime ideals in M is a chain of distinct prime ideals in R, hence $\mathrm{ht}(M) \leq \dim(R)$. Now let

$$P_0 \subset P_1 \subset \cdots \subset P_r$$

be a chain of distinct prime ideals in R. If $P_r \neq M$, then we may add M to the chain, so any chain of distinct prime ideals in R is contained in a chain of distinct prime ideals in M. It follows that $\dim(R) \leq \mathrm{ht}(M)$.

For the second part of the lemma, we notice that R_P is a local ring with maximal ideal $R_P P$, hence

$$\dim(R_P) = \mathrm{ht}(R_P P).$$

To conclude, it is sufficient to observe that $\mathrm{ht}(P) = \mathrm{ht}(R_P P)$. □

The next result is also elementary.

Proposition 1 *A 1-dimensional UFD is a PID. In particular, a Dedekind domain which is not a field and is a UFD is a PID.*

PROOF Let R be a 1-dimensional UFD and P a nontrivial prime ideal in R. Then P has a nonzero element x. Since R is a UFD, we may write

$$x = u p_1^{r_1} \cdots p_n^{r_n},$$

where the p_i are prime elements in R, the r_i are positive integers and u is a unit. Since P is prime, we have $p_i \in P$, for some i, hence we have a chain of distinct prime ideals $(0) \subset (p_i) \subset P$. As $\dim R = 1$, we must have $P = (p_i)$, i.e., P is principal. It follows from Theorem 1 that R is a PID.

As a Dedekind domain which is not a field is 1-dimensional, if it is a UFD, then it is a PID. □

PIDlem1 **Lemma 3** *Let R be an integral domain and $P_1 = (p_1)$, $P_2 = (p_2)$ distinct nontrivial principal prime ideals. Then $P_1 \not\subset P_2$. In particular, a PID which is not a field has dimension 1.*

PROOF Suppose that $P_1 \subset P_2$. Then there exists $a \in R$ such that $p_1 = a p_2$. Since P_1 is a prime ideal, either $p_2 \in P_1$ or $a \in P_1$. In the first case, $P_2 \subset P_1$ and so $P_1 = P_2$, a contradiction. If $a \in P_1$, then we may write $a = b p_1$ and so $p_1 = b p_1 p_2$, which implies that $p_1(1 - b p_2) = 0$. Since R is a domain, either $p_1 = 0$ or $1 - b p_2 = 0$. In the first case we have $P_1 = (0)$, which is a contradiction. In the second case p_2 is a unit and so $P_2 = R$, which is also impossible. It follows that $P_1 \not\subset P_2$.

If R is a PID, then all prime ideals are principal, so no chain of distinct prime ideals can be longer than 1, hence $\dim(R) \leq 1$. Since R is not a field, R has at least one prime ideal, so $1 \leq \dim(R)$, and it follows that $\dim(R) = 1$. □

PIDcor1a **Corollary 2** *In a PID every nonzero prime ideal is maximal.*

PROOF Let R be a PID and P a nonzero prime ideal in R. There exists a maximal ideal M in R containing P. As P and M are principal and prime and $P \subset M$, we must have $P = M$. □

We use Lemma 3 in the next proposition.

PIDprop1 **Proposition 2** *Let R be a UFD and $P \neq (0)$ a prime ideal in R. Then $ht(P) = 1$ if and only if P is principal.*

PROOF Suppose that P is a nonzero prime ideal and let x be a nonzero element of P. Then $x = up_1^{a_1} \cdots p_n^{a_n}$, where u is a unit, the p_i are prime elements and the a_i positive integers. As P is a prime ideal, $p_i \in P$, for some i. Therefore $(0) \subset (p_i) \subset P$. Thus a nonzero prime ideal contains a nonzero principal prime ideal.

Suppose that P is a nonzero prime ideal such that $\mathrm{ht}(P) = 1$. As P contains a nonzero principal prime ideal (p), we have $(0) \subset (p) \subset P$. Given that $\mathrm{ht}(P) = 1$ we have the equality $P = (p)$.

Now suppose that P is principal, with $P = (p)$. If P contains a nonzero prime ideal Q, then Q contains a nonzero principal prime ideal (q) and we have $(q) \subset Q \subset P = (p)$. Applying Lemma 3, we obtain $(q) = (p)$ and so $Q = P$. Thus $\mathrm{ht}(P) = 1$. □

PIDlem1

Dimension of a polynomial ring

First we aim to show that the dimension of a ring R determines bounds on the dimension of the associated polynomial ring $R[X]$. We need a preliminary result.

PIDlemma2

Lemma 4 *Let R be an arbitrary commutative ring. If $Q \subsetneq Q'$ are prime ideals in $S = R[X]$ whose contractions to R are the same, i.e., $P = R \cap Q = R \cap Q'$, then $Q = SP$.*

PROOF First we show that SP is a prime ideal in S, if P is a prime ideal in R. Clearly SP is an ideal. SP is composed of all polynomials in S with coefficients in P. From hereon we will write $P[X]$ for SP. Suppose that $f(X) = \sum_{i=0}^{m} a_i X^i$ and $g(X) = \sum_{j=0}^{n} b_j X^j$ belong to S, with $fg \in P[X]$. If $f \notin P[X]$ and $g \notin P[X]$, then there are coefficients of f and g not in P. Let a_u (resp. b_v) be the first coefficient of f (resp. g) not in P. If $fg(X) = \sum_{k=0}^{m+n} c_k X^k$, then

$$c_{u+v} = a_0 b_{u+v} + a_1 b_{u+v-1} + \cdots + a_{u-1} b_{v+1} + a_u b_v + a_{u+1} b_{v-1} + \cdots + a_{u+v} b_0.$$

All the terms of the sum, with the possible exception of $a_u b_v$, clearly lie in P, as does c_{u+v}. But this implies that $a_u b_v$ lies P. As P is a prime ideal, either a_u or b_v belongs to P, a contradiction. Hence $f \in P[X]$ or $g \in P[X]$ and it follows that $P[X]$ is a prime ideal.

Suppose now that $Q \subsetneq Q'$ are prime ideals in $R[X]$ and $P = R \cap Q = R \cap Q'$. Suppose that $P[X] \neq Q$, i.e., $P[X]$ is properly contained in Q. Then the three ideals $P[X] \cap R$, $R \cap Q$ and $R \cap Q'$ all lie in P, hence outside of the set $U = R \setminus P$, which is a multiplicative set in R, hence in $R[X]$. We deduce that $P[X]$, Q and Q' do not intersect U. We now localise with respect to U and obtain a chain (C) of distinct prime ideals in $U^{-1}(R[X])$

$$U^{-1}(P[X]) \subset U^{-1}Q \subset U^{-1}Q'.$$

In addition, we notice that

$$U^{-1}(R[X]) = (U^{-1}R)[X] = R_P[X] \text{ and } U^{-1}(P[X]) = (U^{-1}P)[X] = R_P P[X],$$

where $R_P P$ is the unique maximal ideal in R_P.

We now note π the canonical projection of $R_P[X]$ onto $R_P[X]/R_P P[X] = (R_P/R_P P)[X]$. Applying π to the chain (C) we obtain a chain (C') of three distinct prime ideals in $(R_P/R_P P)[X]$. However, $(R_P/R_P P)$ is a field, because $R_P P$ is a maximal ideal in R_P and so $(R_P/R_P P)[X]$ is a PID, which is not a field. From Lemma 3 the dimension of such a ring is 1. So we have a contradiction and it follows that $Q = P[X]$. □

PIDlem1

PIDcor2

Corollary 3 *If R is an arbitrary commutative ring and Q' is a prime ideal in $R[X]$, there is at most one other prime ideal Q strictly included in Q' such that $R \cap Q = R \cap Q'$. In particular, if Q' is a nonzero prime ideal in $R[X]$ and $R \cap Q' = (0)$, then there is no nonzero prime ideal Q strictly included in Q' such that $R \cap Q = (0)$.*

PROOF If $P = R \cap Q'$ and $Q \neq Q'$, then $Q = P[X]$. □

We now may consider the bounds on the dimension of a polynomial ring.

Theorem 2 *If R is an arbitrary commutative ring of dimension n, then $R[X]$ is at least $(n+1)$-dimensional and at most $(2n+1)$-dimensional.*

PROOF If

$$P_0 \subset P_1 \subset \cdots \subset P_n \subset R$$

is a chain of distinct prime ideals in R, then

$$R[X]P_0 \subset R[X]P_1 \subset \cdots \subset R[X]P_n \subset R[X]$$

is a chain of distinct prime ideals in $R[X]$. In addition, $R[X]P_n$ is not maximal, because

$$R[X]P_n \subsetneq (R[X]P_n, X) \subsetneq R[X].$$

It follows that $R[X]$ is at least $(n+1)$-dimensional.

We now consider a chain of distinct prime ideals in $R[X]$:

$$Q_0 \subset Q_1 \subset \cdots \subset Q_m \subset R[X].$$

We set $P_i = R \cap Q_i$, for $i = 0, \ldots, m$. Suppose that there are s distinct prime ideals among the P_i. From Corollary 3 PIDcor2 at most two prime ideals Q_i have the same intersection with R. If $2s < m+1$, then there must be at least one P_j which is the contraction of three prime ideals Q_i, contradicting Corollary 3 PIDcor2, hence we have

$$m + 1 \leq 2s \leq 2(n+1) = 2n + 2 \Longrightarrow m \leq 2n + 1,$$

and so

$$n + 1 \leq \dim(R[X]) \leq 2n + 1.$$

This ends the proof. □

Corollary 4 *If R is a PID which is not a field, then* $\dim R[X] = 2$.

PROOF If R is a PID, which is not a field, then $\dim(R) = 1$, so $\dim(R[X])$ is 2 or 3. If the dimension is 3, then there is a chain of distinct prime ideals $(0) = Q_0 \subset Q_1 \subset Q_2 \subset Q_3$. (The ideal Q_3 must be maximal; otherwise Q_3 is properly contained in a maximal ideal, which is prime and so we have a chain of distinct prime ideals whose length is at least 4, a contradiction.) Taking the intersections with R, we obtain a chain of prime ideals $(0) = P_0 \subset P_1 \subset P_2 \subset P_3$ in R. We notice that $P_1 = (0)$. If this is not the case, then from Lemma 3 PIDlem1 we have $P_1 = P_2$, and using Lemma 3 PIDlem1 again we have $P_2 = P_3$. However, from Corollary 3 PIDcor2, we cannot have $P_1 = P_2 = P_3$. Hence $P_1 = (0)$, as claimed.

Next we notice that $P_2 \neq (0)$. If this is not the case, then we have a $Q_1 \subset Q_2$, with $Q_1 \neq Q_2$, and $P_1 = P_2 = (0)$, contradicting Corollary 3 PIDcor2. Hence there is a prime element $p \in R$ such that $P_2 = (p)$.

Then $R[X](p) = R[X]p$ is a prime ideal included in Q_2. If $R[X]p = Q_2$, then, from Proposition 2 PIDprop1, $\mathrm{ht}(Q_2) = 1$, which is impossible, because $\mathrm{ht}(Q_1) \neq 0$ and $\mathrm{ht}(Q_1) < \mathrm{ht}(Q_2)$. Thus we have a chain of distinct prime ideals $R[X]p \subset Q_2 \subset Q_3$ in $R[X]$.

Now $R \cap R[X]p = (p) = P_2$. Also, $P_3 \neq (p)$, because we cannot have a chain of three distinct nonzero prime ideals in $R[X]$ having the same intersection with R (again using Corollary 3 PIDcor2).

Thus P_2 is strictly included in P_3, contradicting Lemma 3. It follows that $\dim(R[X] \neq 3$ and so $\dim(R[X]) = 2$, as claimed. □

We now consider valuation rings. We aim to show that, if R is a 1-dimensional valuation ring, then $\dim(R[X]) = 2$. We begin with two preliminary results.

PIDlem3 **Lemma 5** *Let $S = \{a_1, \ldots, a_n\}$ be a set of elements in a valuation ring R. Then S has a minimal element, i.e., an element a_j which divides all the a_i.*

PROOF In a valuation ring R, if $a, b \in R$, then $a|b$ or $b|a$; thus, if $n = 2$, there is nothing to prove. Suppose now that the result is true up to $n - 1$. Without loss of generality, let us assume that $a_1|a_i$, for $i = 1, \ldots, n-1$. Now $a_1|a_n$ or $a_n|a_1$. In the first case a_1 is minimal and in the second case a_n is minimal. Hence S has a minimal element. □

PIDlem4 **Lemma 6** *If P is a nonzero prime ideal in a 1-dimensional valuation ring R and Q a nonzero prime ideal in $R[X]$ such that*

$$(0) \subset Q \subset P[X],$$

then $Q = P[X]$. (As above, we write $P[X]$ for $R[X]P$.)

PROOF Since Q is a nonzero prime ideal, there is a nonzero polynomial $f(X) \in Q$. From Lemma 6, $f(X)$ has a coefficient which divides all its coefficients. Dividing out by this coefficient we obtain the expression $f(X) = cg(X)$, where $c \in P$ and $g(X) \in R[X]$, with at least one coefficient equal to 1. Then $g(X) \notin P[X]$, because $1 \notin P$. As Q is a prime ideal, $f(X) = cg(X) \in Q$ and $g(X) \notin Q$, we must have $c \in Q$.

Since $c \neq 0$, $R \cap Q$ is a nonzero prime ideal in R. Also,

$$(0) \subset R \cap Q \subset R \cap P[X] = P.$$

As $\dim(R) = 1$, we have $R \cap Q = P$ and so

$$P[X] = R[X](R \cap Q) \subset R[X]Q \subset Q.$$

By hypothesis, $Q \subset P[X]$, hence we have $Q = P[X]$, as required. □

We now may prove the result alluded to above.

Theorem 3 *If R is a 1-dimensional valuation ring, then* $\dim(R[X]) = 2$.

PROOF Because $\dim(R[X]) \leq 3$, no chain of prime ideals in $R[X]$ can have a length greater than 3. We aim to show that even this is not possible. Let

$$(0) = Q_0 \subset Q_1 \subset Q_2 \subset Q_3$$

be a chain of distinct prime ideals in $R[X]$. We set $P_i = R \cap Q_i$. If $P_1 \neq (0)$, then $P_1 = P_2 = P_3$, because $\dim(R) = 1$. As this is impossible $P_1 = (0)$. Now we show that $P_2 \neq (0)$. If $P_2 = (0)$, then we have $P_0 = P_1 = P_2$, which is impossible, so $P_2 \neq (0)$.

We claim that $R[X]P_2 = Q_2$. Clearly, $R[X]P_2 \subset Q_2$. Because $\dim(R) = 1$, we must have $P_3 = P_2$. Also,

$$R \cap R[X]P_2 = R \cap R[X](R \cap Q_2) = R \cap Q_2 = P_2.$$

If $R[X]P_2$ is a proper subset of Q_2, then we have a chain of three distinct prime ideals in $R[X]$ whose intersection with R is P_2. As this is impossible, we must have $R[X]P_2 = Q_2$. However,

$Q_1 \subset Q_2$, so, by Lemma PIDlem4 6, $Q_1 = R[X]P_2 = Q_2$, a contradiction. It follows that $\dim(R[X]) = 2$. □

Remark If R is a discrete valuation ring, then it is a PID, so it has dimension 1. It follows from the result we have just proved that $\dim(R[X]) = 2$.

Radicals

We recall a definition. The spectrum of ring, written $\mathrm{Spec}(R)$, is the set of prime ideals in R.

There is a natural question which arises, namely is it possible to characterize the intersection of the prime ideals (resp. maximal ideals) in a ring. This is in fact the case. The first intersection is called the nilradical, written $N(R)$, and the second the Jacobson radical, written $J(R)$. Clearly, $N(R) \subset J(R)$.

PIDthm2 **Theorem 4** *The nilradical of a ring R is composed of the nilpotent elements in R, namely those elements $x \in R$ for which there exists $n \in \mathbf{N}^*$ such that $x^n = 0$.*

PROOF Let X be the set of nilpotent elements in R. Suppose that P is a prime ideal in R and $x \in X$. There exists $n \in \mathbf{N}^*$ such that $x^n = 0 \in P$. Since P is prime, we have $x \in P$. Thus $X \subset N(R)$.

We now consider the converse. It is sufficient to show that $a \notin X$ implies that $a \notin N(R)$, and for this it is sufficient to show that there is a prime ideal which does not contain a. Let $a \notin X$ and S be the set of ideals in R which do not contain a positive power of a. S is not empty: Since a is not nilpotent, no positive power of a lies in (0), so (0) belongs to S. We order S by inclusion. The union of the ideals in a chain clearly lies in S, thus a chain has a maximum. From Zorn's lemma, S has a maximal element, which we note M.

We claim that M is prime. If this is not the case, then there exist $x, y \notin M$ such that $xy \in M$. M is strictly contained in the ideal $(M, x) = M + (x)$, which does not belong to S, because M is maximal. Hence there exists $n \in \mathbf{N}^*$ such that $a^n \in (M, x)$. In the same way, there exists $m \in \mathbf{N}^*$ such that $a^m \in (M, y) = M + (y)$. Then

$$a^{n+m} = a^n a^m = (m_1 + r_1 x)(m_2 + r_2 y) = m_1 m_2 + m_1 r_2 y + r_1 x m_2 + r_1 x r_2 y,$$

where $r_1, r_2 \in R$ and $m_1, m_2 \in M$. As $xy \in M$, $a^{n+m} \in M$, which contradicts the fact that $M \in S$. It follows that M is a prime ideal, as claimed. Since M contains no positive power of a, a does not belong to M. Hence there exists a prime ideal which does not contain a and so $a \notin N(R)$. Therefore $N(R) \subset X$ and we conclude that $N(R) = X$ □

We now turn to the Jacobson radical.

Theorem 5 *The Jacobson radical of a ring R is composed of those elements $x \in R$ such that $1 - xy$ is a unit for all $y \in R$.*

PROOF Suppose that $x \in J(R)$ and that $1 - xy$ is a nonunit for some $y \in R$. Since $1 - xy$ is a nonunit, there is a maximal ideal M which contains $1 - xy$. As $x \in J(R)$, $xy \in M$ and so $1 = (1 - xy) + xy \in M$, which is impossible because M is a proper ideal in R. Therefore $1 - xy$ is a unit for all $y \in R$.

We now consider the converse. Suppose that $x \notin J(R)$. Then there is a maximal ideal M which does not contain x. We have

$$R = M + (x) = \{m + xy : m \in M, y \in R\}.$$

In particular, $1 = m + xy$, for some $y \in R$. Hence $m = 1 - xy$, which is a nonunit, because M is a proper ideal. □

Example Let F be a field, $R = \prod_{i=1}^{\infty} F$ and M_j the ideal in R which is F on every coordinate other than j and 0 on the jth coordinate. Each M_j is a maximal ideal and the intersection of the M_j is the zero ideal, which is not maximal. It follows that $J(R)$ is not maximal. As the zero ideal is not prime, $J(R)$ is not even prime. This shows that in general the Jacobson radical is not prime. Given that the nilradical is contained in the Jacobson radical, we see that the nilradical is in general not prime.

Remark The nilradical may be strictly contained in the Jacobson radical. Here is an example. Let R be a local integral domain which is not a field. (An example is $R = F[[X]]$, with F a field, since the nonzero ideals of $F[[X]]$ are of the form $F[[X]]X^n$, for some $n \geq 1$.) If M is its unique maximal ideal, then $N(R) = (0)$, because $(0) \in \mathrm{Spec}(R)$, and $J(R) = M$.

We say that an element a in a commutative ring R is quasi-regular, if $1 - a$ is a unit. Clearly, all the elements in the Jacobian radical $J(R)$ are quasi-regular. However, we can say a little more.

Theorem 6 *If an ideal I is composed entirely of quasi-regular elements, then I is included in $J(R)$.*

PROOF Let I be an ideal composed entirely of quasi-regular elements. If $a \in I \setminus J(R)$, then a does not belong to some maximal ideal M. As M is maximal, we have $R = I + M$, so $1 = b + c$, with $b \in I$ and $c \in M$. However, b is quasi-regular, so $c = 1 - b$ is a unit, which is impossible. It follows that $I \subset J(R)$. □

We may generalize the nilradical. For an ideal I in a ring R, we define the radical of I, which we will note $r(I)$, to be the intersection of the prime ideals in R containing I. Then $r((0)) = N(R)$. The proof of the following characterization of the radical is analogous to the proof of Theorem 4.

Theorem 7 *$r(I)$ is the set of elements $x \in R$ such that $x^n \in I$, for some $n \in \mathbf{N}^*$.*

PROOF Let X be the set of elements $x \in R$ such that $x^n \in I$, for some $n \in \mathbf{N}^*$. Suppose that P is a prime ideal in R containing I and that $x \in X$. There exists $n \in \mathbf{N}^*$ such that $x^n \in I \subset P$. Since P is prime, we have $x \in P$. Thus $X \subset r(I)$.

We now consider the converse. It is sufficient to show that $a \notin X$ implies that $a \notin r(I)$, and for this it is sufficient to show that there is a prime ideal P containing I such that $a \notin P$. Let $a \notin X$ and S be the set of ideals in R containing I which do not contain a positive power of a. We order S by inclusion. As no power of a belongs to I, I belongs to S, so S is nonempty. The union of the ideals in a chain clearly lies in S, thus a chain has a maximum. From Zorn's lemma, S has a maximal element, which we note M.

We claim that M is prime. If this is not the case, then there exist $x, y \notin M$ such that $xy \in M$. M is strictly contained in the ideal $(M, x) = M + (x)$, which does not belong to S, because M is maximal. Hence there exists $n \in \mathbf{N}^*$ such that $a^n \in (M, x)$. In the same way, there exists $m \in \mathbf{N}^*$ such that $a^m \in (M, y) = M + (y)$. Then

$$a^{n+m} = a^n a^m = (m_1 + r_1 x)(m_2 + r_2 y) = m_1 m_2 + m_1 r_2 y + r_1 x m_2 + r_1 x r_2 y,$$

where $r_1, r_2 \in R$ and $m_1, m_2 \in M$. As $xy \in M$, $a^{n+m} \in M$, which contradicts the fact that $M \in S$. It follows that M is a prime ideal, as claimed. As M contains no positive power of a, a does not belong to M. Hence there exists a prime ideal containing I which does not contain a and so $a \notin r(I)$. Thus $r(I) \subset X$ and we conclude that $r(I) = X$ □

For ideals whose radical is finitely generated we have the following result:

Proposition 3 *If I is an ideal in a ring R whose radical $r(I)$ is finitely generated, then there a positive power of $r(I)$ included in I.*

PROOF Let $r(I) = (x_1, \ldots, x_k)$. For each x_i there exists $n_i \in \mathbf{N}^*$ such that $x_i^{n_i} \in I$. We set $n = n_1 + \cdots + n_k$. By the multinomial theorem, $r(I)^n$ is generated by the elements of the form $x_1^{r_1} \cdots x_k^{r_k}$, with $r_1 + \cdots + r_k = n$. For each such element, there exists $r_i \geq n_i$, for some i (otherwise $r_1 + \cdots + r_k < n$). Hence $x_1^{r_1} \cdots x_k^{r_k} \in I$. It follows that $r(I)^n \in I$. □

PIDcor2a **Corollary 5** *If I is an ideal in a noetherian ring R, then there a positive power of the radical $r(I)$ included in I.*

PROOF Every ideal in a noetherian ring is finitely generated. □

We have seen above that in general the nilradical is not equal to the Jacobson radical. However, for certain rings this is the case. We recall that a ring is artinian if any descending chain of ideals becomes stationary after a certain point. We will show that for such rings the nilradical is equal to the Jacobson radical. We need two preliminary results.

PIDlem5 **Lemma 7** *If R is an artinian integral domain, then R is a field.*

PROOF Let a be a nonzero element of R. As R is artinian, the descending chain of ideals $(a) \supset (a^2) \supset \cdots$ is stationary after a certain point: there exists $n \in \mathbf{N}^*$ such that $(a^n) = (a^{n+1}) = \cdots$. As $a^n \in (a^{n+1})$, there exists $b \in R$ such that $a^n = a^{n+1} b$, which implies that $1 = ab$, so a is invertible. Thus R is a field. □

PIDlem6 **Lemma 8** *If R is an artinian ring and I an ideal in R, then R/I is an artinian ring.*

PROOF Let $\bar{I}_0 \supset \bar{I}_1 \supset \cdots$ be a descending chain of ideals in R/I. The ideals $\bar{I}_i$ have the form $I_i + I$ and the I_i form a descending chain in R. As R is artinian, this chain becomes stationary after a certain point, hence so does the chain $\bar{I}_0 \supset \bar{I}_1 \supset \cdots$. Therefore R/I is artinian. □

PIDthm3 **Theorem 8** *A prime ideal in an artinian ring is maximal. Hence the nilradical and the Jacobian radical are identical in an artinian ring.*

PROOF Let R be an artinian ring and P a prime ideal in R. Then R/P is an integral domain and artinian by Lemma PIDlem6 8. From Lemma PIDlem5 7, R/P is a field and so P is maximal. It follows that the nilradical of R is equal to its Jacobson radical. □

Remark Suppose that R is an artinian ring. If R is an integral domain, then R is a field, so the only prime ideal is (0), which implies that $\dim(R) = 0$. On the other hand, if R is not an integral domain and P is a prime ideal in R, then P is maximal and the only chain containing P is composed of the unique element P. It follows that all chains of distinct prime ideals have a single element. Hence $\dim(R) = 0$. Therefore the dimension of an artinian ring is always 0.

Finite intersections and unions

We first consider the case where a finite intersection of ideals is contained in a prime ideal.

PIDprop2 **Proposition 4** *Let $I_1, \ldots, I_n$ be ideals in a ring R and P a prime ideal in R such that $\cap_{i=1}^n I_i \subset P$. Then there is an index j such that $I_j \subset P$. If $\cap_{i=1}^n I_i = P$, then $I_j = P$.*

PROOF If the statement is not true, then for each i there exists $x_i \in I_i$ such that $x_i \notin P$. The product of the x_i belongs to the intersection of the I_i and so to P. However, P is a prime ideal, hence there exists some index j such that $x_j \in P$, which is a contradiction. Hence $I_j \subset P$.

If $\cap_{i=1}^n I_i = P$, then $P \subset I_j$, so $P = I_j$. □

We now consider the case where an ideal is contained in a finite union of prime ideals. This is more difficult.

PIDthm2a **Theorem 9** *(prime avoidance lemma) Let R be a ring and $I, P_1, \ldots, P_n$ be ideals in R, with P_i prime for $i > 2$. If I is contained in the union of the P_i, then there is an index i such that $I \subset P_i$.*

PROOF We prove the result by induction on n. If $n = 1$, then there is nothing to prove. Suppose that $n = 2$ and that the result is false. Then $I \subset P_1 \cup P_2$ and there exists $x_1 \in I \setminus P_1$ and $x_2 \in I \setminus P_2$. As $x = x_1 + x_2 \in I$, we have $x \in P_1$ or $x \in P_2$. However, if $x \in P_1$, then $x_1 = x - x_2 \in P_1$ (since $x_2 \in I \setminus P_2$ implies that $x_2 \in P_1$), which is a contradiction, so $x \notin P_1$. In the same way, $x \notin P_2$. Hence $x \notin P_1 \cup P_2$, which contradicts the fact that $I \subset P_1 \cup P_2$. Hence the result is true for $n = 2$.

Suppose now that $n > 2$ and that the result is true up to $n - 1$, but that the result is false for n. We may assume that I is not contained in any collection of $n - 1$ of the P_i. (If this were the case, then, by the induction hypothesis, I would be contained in one of the P_i.) Thus, for each i, there exists

$$x_i \in I \setminus \cup_{j \neq i} P_j.$$

Now $x_1 \cdots x_{n-1} \in P_1 \cap \cdots \cap P_{n-1}$ and $x_n \notin P_1 \cup \cdots \cup P_{n-1}$. Let $x = (x_1 \cdots x_{n-1}) + x_n$. We aim to show that $x \notin P_1 \cup \cdots \cup P_n$, contradicting the fact that $I \subset P_1 \cup \cdots \cup P_n$. If x belongs to $P_1 \cup \cdots \cup P_{n-1}$, then so does x_n, which is not true, so x does not belong to $P_1 \cup \cdots \cup P_{n-1}$. For $i = 1, \ldots, n-1$, $x_i \notin P_n$ ($x_i \in P_n \Longrightarrow x_i \in \cup_{j \neq i} P_j$), hence $x_1 \cdots x_{n-1} \notin P_n$, because P_n is prime. But $x_n \in P_n$, so $x \notin P_n$. Thus $x \in I$ and $x \notin P_1 \cup \cdots \cup P_n$, a contradiction. It follows that the result is true for n. □

Remark The contrepositive statement of the theorem goes as follows: Let R be a ring and $I, P_1, \ldots, P_n$ be ideals in R, with P_i prime for $i > 2$. If I is not a subset of one of the P_i, then I is not contained in the union of the P_i. Thus there is an element x in I which belongs to none of the ideals P_i. We could say that x "avoids" the P_i. This is the origin of the term "prime avoidence lemma".

Further properties of artinian (and noetherian) rings

PIDprop3

Proposition 5 *If R is an artinian ring, then the nilradical $N(R)$ is nilpotent, i.e., there exists $n \in \mathbf{N}^*$ such that $N(R)^n = (0)$. As the Jacobson radical is equal to the nilradical, the Jacobson radical is also nilpotent.*

PROOF For simplicity, let us write N for $N(R)$. As R is artinian, the decreasing sequence $N \supset N^2 \supset \cdots$ becomes stationary after a certain point, i.e., there exists $n \in \mathbf{N}^*$ such that $N^n = N^{n+1} = \cdots$. We claim that $I = N^n$ is the zero ideal.

Suppose that $I \neq (0)$ and let S be the set of ideals J such that $IJ \neq (0)$. Clearly $R \in S$, so S is nonempty. Since R is artinian, any descending chain has a minimum, so, by Zorn's lemma, S has a minimal element K. As $IK \neq (0)$, there exists $a \in K$ such that $Ia \neq (0)$, i.e., $I(a) \neq (0)$. By minimality, we have $(a) = K$. However, $N^n = N^{2n}$ implies that $I = I^2$, hence $Ia = (II)a = I(Ia)$ and so $Ia \in S$. In addition, $Ia \subset (a) = K$; by minimality, $Ia = (a)$.

Thus, there exists $x \in I$ such that $xa = a$, from which we deduce that $x^2a = x(xa) = xa = a$. By induction we obtain $x^na = a$, for all $n \in \mathbf{N}^*$. However, $x \in I$ implies that $x \in N$ and so $x^s = 0$, for some $s \in \mathbf{N}^*$, which implies that $a = x^sa = 0$, which is a contradiction, because $Ia \neq (0)$. It follows that $I = N^n = (0)$, as claimed. □

We now consider the number of maximal ideals in an artinian ring, or equivalently the number of prime ideals.

PIDprop4

Proposition 6 *If R is an artinian ring, then the number of maximal ideals in R is finite.*

PROOF Let S be the set of all finite intersections of maximal ideals in R. A descending chain has a minimum, because R is artinian, so by Zorn's lemma, S has a minimal element, say $M_1 \cap \cdots \cap M_n$. We claim that the maximal ideals in R are the ideals $M_1, \ldots, M_n$.

If M is a maximal ideal, then $M_1 \cap \cdots \cap M_n \cap M \subset M_1 \cap \cdots \cap M_n$. By minimality, $M_1 \cap \cdots \cap M_n \cap M = M_1 \cap \cdots \cap M_n$, hence $M_1 \cap \cdots \cap M_n \subset M$. From Proposition 4 (PIDprop2) there is an index i such that $M_i \subset M$. As M_i is maximal, we have $M_i = M$. □

It is not so that a noetherian ring is necessarily an artinian ring. We only need to consider the ring of integers $\mathbf{Z}$, which is noetherian, but not artinian. However, an artinian ring is noetherian, as we will presently show.

Lemma 9 *A vector space V over a field F is artinian (resp. noetherian) if and only if* $\dim V < +\infty$.

PROOF Suppose that $\dim V = n < +\infty$ and let C be a descending chain of subspaces in V. If C does not stabilize, then C contains an infinite subchain $V_0 \supset V_1 \supset \cdots$ of distinct subspaces. Thus $n \geq \dim V_0 > \dim V_1 > \cdots$ is an infinite decreasing sequence of nonnegative integers, which is impossible. Hence R is artinian.

Now suppose that $\dim V = +\infty$. We set $V_0 = V$ and take $v_1 \in V_0$, with $v_1 \neq 0$. Then $\langle v_1 \rangle$ has a complement V_1 in V_0 (see Appendix). We now choose $v_2 \in V_1$, with $v_2 \neq 0$. Then $\langle v_2 \rangle$ has a complement V_2 in V_1. We now have $V_2 \subset V_1 \subset V_0$, where the inclusions are strict. Continuing in the same way, we obtain an infinite descending chain of distinct subspaces of V, thus V is not artinian.

Once again suppose that $\dim V = n < +\infty$. If C is an ascending chain of subspaces which does not stabilize, then C contains an infinite subchain $V_0 \subset V_1 \subset \cdots$ of distinct subspaces, with $\dim V_0 < \dim V_1 < \cdots \leq n$, which is clearly imposible. So every chain of subspaces stabilizes and V is noetherian.

Let us now suppose that $\dim V = +\infty$. If V_i is a subspace, then we can find a subspace V_{i+1} strictly containing V_i. Hence we can construct an ascending chain of subspaces which does not stabilize, and so V is not noetherian. □

PIDcor3 **Corollary 6** *A vector space is artinian if and only if it is noetherian.*

We recall the following fundamental result:

PIDthm4 **Theorem 10** *If R is a commutative ring, M an R-module and N a submodule of M, then M is artinian (resp. noetherian) if and only if M/N and N are both artinian (resp. noetherian).*

PIDlem7 **Lemma 10** *Let R be a commutative ring and suppose that there are (not necessarily) distinct maximal ideals $M_1, \ldots, M_s$ such that $M_1 \cdots M_s = (0)$. Then R is artinian if and only if R is noetherian.*

PROOF Consider the chain of R-modules

$$R \supset M_1 \supset M_1 M_2 \supset \cdots \supset M_1 M_2 \cdots M_s = (0).$$

For $i = 1, \ldots, s$, R/M_i is a field and $M_1 \cdots M_{i-1}/M_1 \cdots M_i$ an R/M_i-vector space. From Corollary 6, $M_1 \cdots M_{i-1}/M_1 \cdots M_i$ is artinian if and only if it noetherian. We notice that the vector spaces $M_1 \cdots M_{i-1}/M_1 \cdots M_i$ are also R-modules, hence they are artinian R-modules if and only if they are noetherian R-modules.

Suppose now that the ring R is artinian. From Theorem 10, R/M_1 and M_1 are artinian. Applying the theorem again, we see that M_1/M_1M_2 and M_1M_2 are artinian. Continuing in the same way, we obtain that the modules $M_1 \cdots M_{i-1}/M_1 \cdots M_i$ are all artinian, and in particular, with $i = s$, that $M_1 \cdots M_{s-1}$ is artinian and so noetherian.

We now use Theorem 10 again, but in a 'reverse' direction. Since $M_1 \cdots M_{s-2}/M_1 \cdots M_{s-1}$ and $M_1 \cdots M_{s-1}$ are noetherian, the module $M_1 \cdots M_{s-2}$ is noetherian. Continuing in the same way, we find that R/M_1 and M_1 are both noetherian, hence R is a noetherian R-module, and so a noetherian ring.

In an analogous manner, we show that if R is noetherian, then R is artinian. □

We now may prove the result alluded to above.

Theorem 11 *If R is an artinian ring, then R is noetherian.*

PROOF From Proposition 6 the number of maximal ideals in R is finite. Also, by Proposition 5, the Jacobson radical is nilpotent. Thus there is a finite number of maximal ideals whose product is (0). Now, using Lemma 10, we obtain that R is noetherian. □

We have seen above that a noetherian ring is not necessarily artinian. However, if we suppose that the dimension of R is 0, then this is the case. To prove this, we begin by introducing the notion of an irreducible ideal. An ideal I in a commutative ring R is irreducible, if $I = J \cap K$, for ideals J and K, implies that $I = J$ or $I = K$.

Proposition 7 *A prime ideal I in a ring R is irreducible.*

PROOF This is a direct consequence of Proposition 4. □

It is not difficult to determine the irreducible ideals in the ring of integers $\mathbf{Z}$.

Proposition 8 *An nonzero ideal $(a) \subset \mathbf{Z}$ is irreducible if and only if $(a) = (p^n)$, for some prime number p and nonnegative integer n.*

PROOF Suppose that $(p^n) = (x) \cap (y)$. Then $x|p^n$ and $y|p^n$, which implies that $x = p^k$ and $y = p^l$, with $k, l \leq n$. Without loss of generality, suppose that $k \leq l$. Then $p^k|p^l$, which implies that $(y) \subset (x)$, which in turn implies that $(x) \cap (y) = (y)$.

Suppose now that $(a) \neq (p^n)$, for some prime number p and nonnegative integer n. Then we may set $a = p_1^{n_1} \cdots p_s^{n_s}$, where the p_i are $s > 1$ primes and the n_i positive integers. We have $(a) = (p_1^{n_1}) \cap (p_2^{n_2} \cdots p_s^{n_s})$. As $(a) \neq (p_1^{n_1})$ and $(a) \neq (p_2^{n_2} \cdots p_s^{n_s})$, (a) is not irreducible. □

In noetherian rings irreducible ideals play an important role.

PIDprop5 **Proposition 9** *Let R be a noetherian ring.*

- **1.** *An ideal in R is a finite intersection of irreducible ideals.*
- **2.** *If I is an irreducible ideal in R, then the radical $r(I)$ is a prime ideal.*

PROOF **1.** Suppose that the result is false. Let S be the set of ideals which are not finite intersections of irreducible ideals. By hypothesis S is nonempty. As R is noetherian, any chain in S has a maximum, so, by Zorn's lemma, S has a maximal element, which we note M. As $M \in S$, M is not irreducible, so we can write $M = J \cap K$, where J and K are ideals which both properly contain M. Given that M is maximal in S, J and K do not belong to S and so are finite intersections of irreducible ideals. However, $M = J \cap K$, which implies that M is a finite intersection of irreducible ideals, a contradiction. Hence S is empty and the result follows.

2. Let us first consider the case where $I = (0)$. Then $r(I) = N(R)$. If $xy \in N(R)$, then there exists $n \in \mathbf{N}^*$ such that $(xy)^n = 0$. If $y \notin N(R)$, then $y^n \neq 0$. We aim to show that this implies that there exists $t \in \mathbf{N}^*$ such that $x^t = 0$ and so that $x \in N(R)$.

We have the chain of ideals

$$ann(x^n) \subset ann(x^{2n}) \subset ann(x^{3n}) \subset \cdots$$

(We recall that $ann(x^{sn})$ is the set of annihilators of x^{sn}, i.e., the elements $r \in R$ such that $rx^{sn} = 0$.) As R is noetherian, this chain stabilizes: suppose that $ann(x^{mn}) = ann(x^{(m+1)n}) = \cdots$.

We claim that $(x^{mn}) \cap (y^n) = (0)$. If $a \in (y^n)$, then there exists $a' \in R$ such that $a = a'y^n$ and so $ax^n = a'y^n x^n = 0$. Also, if $a \in (x^{mn})$, then there exists $b \in R$ such that $a = bx^{mn}$. Thus we have

$$0 = ax^n = bx^{mn}x^n = bx^{(m+1)n} \Longrightarrow b \in ann(x^{(m+1)n}) = ann(x^{mn}) \Longrightarrow bx^{mn} = 0.$$

Therefore $(x^{mn}) \cap (y^n) \subset (0)$. Given that $(0) \subset (x^{mn}) \cap (y^n)$, we deduce that $(0) = (x^{mn}) \cap (y^n)$. As (0) is irreducible and $(y^n) \neq (0)$, we have $(x^{mn}) = (0)$ and so $x^{mn} = 0$, which implies that $x \in N(R)$. Hence $N(R)$ is a prime ideal.

We now consider the case where I is a general ideal. We notice that R/I is noetherian and that the nilradical $N(R/I)$ of R/I is $r(I)/I$. If I is irreducible, then so is $(\bar{0}) = I/I$, hence $r(I)/I$ is a prime ideal in R/I and it follows that $r(I)$ is a prime ideal in R. □

We may now prove the result mentioned above, namely

Theorem 12 *If R is a noetherian ring whose dimension* $\dim(R)$ *is 0, then R is artinian.*

PROOF Let R be a noetherian ring. If $\dim(R) = 0$, then every prime ideal is maximal. From Proposition 9, the ideal (0) is a finite intersection of irreducible ideals, say $(0) = I_1 \cap \cdots \cap I_t$. Moreover, using Proposition 9 again, we see that the radical $r(I_i)$ of each ideal I_i is prime and so maximal. Let us set $r(I_i) = M_i$. From Corollary 5, there is a positive integer n_i such that $M_i^{n_i} \subset I_i$. Then we have

$$(0) \subset M_1^{n_1} \cdots M_t^{n_t} \subset I_1 \cdots I_t \subset I_1 \cap \cdots \cap I_t = (0),$$

hence (0) is a finite product of maximal ideals. Applying Lemma 10, we obtain the desired result, namely that R is artinian. □

Appendix

In finite-dimensional vector spaces there is no difficulty in seeing that any vector subspace has a complement. We only need to take a basis of the vector subspace and complete it to a basis of the vector space. In infinite-dimensional vector spaces this is more difficult. Here we give a proof which covers all cases.

Theorem 13 *Let V be a vector space over a field F and W a vector subspace in V. Then W has a complement W' in V.*

PROOF Let $\mathcal{S}$ be the set of vector subspaces of V whose intersection with W is $\{0\}$. As the zero subspace belongs to $\mathcal{S}$, the set $\mathcal{S}$ is nonempty. $\mathcal{S}$ may be ordered by inclusion. Let $\mathcal{C} = \{U_a\}_{a \in A}$ be a chain in $\mathcal{S}$ and U the span of the elements in $\mathcal{C}$. We claim that U is a member of $\mathcal{S}$. By definition, U is a subspace of V, so we only need to show that $W \cap U = \{0\}$. If $x \in W \cap U$, then x may be written

$$x = \sum_{k=1}^{n} a_k m_k,$$

with $a_k \in F$ and $m_k \in U_{a_k}$, for some $a_k \in A$. Since $\mathcal{C}$ is a chain of subsets, there exists $b \in A$ such that $m_1, \ldots, m_n \in U_b$, hence x is a linear combination of elements in U_b and so belongs to U_b. As $W \cap U_b = \{0\}$, we have $x = 0$ and it follows that

$$W \cap U = \{0\}.$$

We have shown that the chain $\mathcal{C}$ has an upper bound. Thus every chain in $\mathcal{S}$ has an upper bound and we may apply Zorn's lemma: there exists a maximal element W' in $\mathcal{S}$. We aim to show that W' is a complement of W in V.

Since $W' \in \mathcal{S}$, we have $W \cap W' = \{0\}$. It remains to show that $W + W' = V$. If $W + W' \neq V$, then there exists $x \in V \setminus \{W + W'\}$. As $0 \in W + W'$, the element x is nonzero. We claim that the vector subspace $W' + \langle x \rangle$ belongs to $\mathcal{S}$. If $w' + ax \in W$, where $w' \in W'$ and $a \in F$, then $ax \in W + W'$. If $a \neq 0$, then $x = \frac{1}{a} ax \in W + W'$, a contradiction, hence $a = 0$ and so $w' \in W$. But then $w' \in W \cap W' = \{0\}$ and so $w' = 0$. It follows that the vector subspace $W' + \langle x \rangle$ is a member of $\mathcal{S}$, as claimed. However, this contradicts the maximality of W'. We have shown that $W + W' = V$, as required. □