1

Rings, homomorphisms, ideals

Our reader does not have to be familiar with commutative rings but should know their definition. Our rings always have an identity element 1. When necessary we write 1_A for the identity element of A. The zero ring $A = \{0\}$ is the only ring such that $1_A = 0$. In the first two sections we recall the really basic facts about ideals and homomorphisms (one of the reasons for doing so is because we need to agree on notation). From section 3 on, we begin to think about algebraic geometry. Prime and maximal ideals are the heart of the matter. Zariski topology, the radicals and comaximal ideals are henceforth treated. Our last section is a first approach to unique factorization domains (UFDs) (the proof of an essential theorem is postponed to chapter 7).

Examples 1.1

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are rings. Each of them is a subring of the next.
2. A commutative field K, with identity element, is a non-zero ring such that $K \setminus \{0\}$ is a multiplicative group.
3. The polynomial ring $K[X_1, ..., X_n]$ is a ring of which $K[X_1, ..., X_{n-1}]$ is a subring.
4. If A is a ring then $A[X_1, ..., X_n]$ is a ring of which $A[X_1, ..., X_{n-1}]$ is a subring.
5. If A and B are two rings, the product $A \times B$ has a natural ring stucture
$$(a, b) + (a', b') = (a + a', b + b') \quad \text{and} \quad (a, b)(a', b') = (aa', bb').$$

Exercises 1.2

1. If K and K' are two fields, verify that the ring $K \times K'$ is not a field.
2. Let p be a prime number. Denote by $\mathbb{Z}_{(p)}$ the subset of $\mathbb{Q}$ consisting of all n/m such that $m \notin p\mathbb{Z}$. Verify that $\mathbb{Z}_{(p)}$ is a subring of $\mathbb{Q}$.

3. Let $x = (x_1, ..., x_n) \in K^n$ be a point. Verify that the set of all P/Q, with $P, Q \in K[X_1, ..., X_n]$, and $Q(x_1, ..., x_n) \neq 0$, is a subring of the field $K(X_1, ..., X_n)$.

Definition 1.3 *Let A and B be rings. A (ring) homomorphism $f : A \to B$ is a set application such that for all $x, y \in A$.*

$$f(1_A) = 1_B, \quad f(x + y) = f(x) + f(y) \quad \text{and} \quad f(xy) = f(x)f(y).$$

An A-algebra is a ring B with a ring homomorphism $f : A \to B$.

The composition of two composable homomorphisms is clearly a homomorphism.

1.1 Ideals. Quotient rings

Proposition 1.4 *The kernel* $\ker f = f^{-1}(0)$, *of a ring homomorphism $f : A \to B$ is a subgroup of A such that*

$$(a \in \ker f \quad \text{and} \quad x \in A) \quad \Rightarrow \quad ax \in \ker f.$$

This is obvious.

Definition 1.5 *A subgroup $\mathcal{I}$ of a ring A is an ideal of A if*

$$(a \in \mathcal{I} \quad \text{and} \quad x \in A) \quad \Rightarrow \quad ax \in \mathcal{I}.$$

If $\mathcal{I} \neq A$, we say that $\mathcal{I}$ is a proper ideal.

Examples 1.6

1. The kernel of a ring homomorphism $f : A \to B$ is an ideal of A.
2. If $n \in \mathbb{Z}$, then $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.
3. Let $a \in A$. The set aA of all multiples of a is an ideal of A.
4. More generally, let a_i, with $i \in E$, be elements in A. The set of all linear combinations, with coefficients in A, of the elements a_i is an ideal. We say that the elements a_i, $i \in E$, form a system of generators of (or generate) this ideal, which we often denote by $((a_i)_{i \in E})$.

As an obvious but important remark we note that all ideals contain 0.

Exercise 1.7 Show that a ring A is a field if and only if (0) is the unique proper ideal of A.

Theorem 1.8 *Let $\mathcal{I}$ be an ideal of A and $A/\mathcal{I}$ the quotient group of equivalence classes for the relation $a \sim b \iff a - b \in \mathcal{I}$. Then $A/\mathcal{I}$ has a ring structure such that the class map $\mathrm{cl} : A \to A/\mathcal{I}$ is a ring homomorphism (obviously surjective) with kernel $\mathcal{I}$.*

Proof It is obvious that $\mathrm{cl}(a+b)$ and $\mathrm{cl}(ab)$ only depend on $\mathrm{cl}(a)$ and $\mathrm{cl}(b)$. Defining then

$$\mathrm{cl}(a) + \mathrm{cl}(b) = \mathrm{cl}(a+b) \quad \text{and} \quad \mathrm{cl}(a)\mathrm{cl}(b) = \mathrm{cl}(ab),$$

the theorem is proved. □

Definition 1.9 *The ring $A/\mathcal{I}$ is the quotient ring of A by the ideal $\mathcal{I}$.*

Example 1.10 If $n \in \mathbb{Z}$, the quotient ring (with $|n|$ elements) $\mathbb{Z}/n\mathbb{Z}$ is well known.

Exercise 1.11 Let K be a field. Show that the composition homomorphism

$$K[Y] \xrightarrow{\mathrm{i}} K[X,Y] \xrightarrow{\mathrm{cl}} K[X,Y]/XK[X,Y]$$

is an isomorphism (i is the natural inclusion and cl the class application).

Let B be a quotient of $A[X_1, ..., X_n]$. The obvious composition homomorphism $A \to B$ gives to B the structure of an A-algebra. We note that any element in B is a combination, with coefficients in A, of products of the elements $\mathrm{cl}(X_1), ..., \mathrm{cl}(X_n) \in B$. These elements generate B as an A-algebra.

Definition 1.12 *A quotient ring B of a polynomial ring $A[X_1, ..., X_n]$ over a ring A is called an A-algebra of finite type or a finitely generated A-algebra.*

Putting $x_i = \mathrm{cl}(X_i) \in B$, we denote B by $A[x_1, ..., x_n]$ and we say that $x_1, \ldots, x_n$ generate B as an A-algebra.

Clearly a quotient of an A-algebra of finite type is an A-algebra of finite type.

Theorem 1.13 *(The factorization theorem)*

Let $f : A \to B$ be a ring homomorphism. There exists a unique injective ring homomorphism $g : A/\ker f \to B$ such that the following diagram is commutative:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow \mathrm{cl} & \nearrow^{g} & \\ A/\ker f & & \end{array}$$

Furthermore f is surjective if and only if g is an isomorphism.

Proof One verifies first that $f(a)$ only depends on $\mathrm{cl}(a) \in A/\ker f$. If we put then $g(\mathrm{cl}(a)) = f(a)$, it is clear that g is a well-defined injective homomorphism. The rest of the theorem follows easily. □

The proof of the following proposition is straightforward and left to the reader.

Proposition 1.14 *Let A be a ring and $\mathcal{I}$ an ideal of A.*

(i) *If $\mathcal{J}$ is an ideal of $A/\mathcal{I}$, then $\mathrm{cl}^{-1}(\mathcal{J})$ is an ideal of A containing $\mathcal{I}$.*
(ii) *If $\mathcal{I}'$ is an ideal of A containing $\mathcal{I}$, then $\mathrm{cl}(\mathcal{I}')$ is an ideal of $A/\mathcal{I}$ (denoted $\mathcal{I}'/\mathcal{I}$).*
(iii) *One has $\mathrm{cl}^{-1}(\mathrm{cl}(\mathcal{I}')) = \mathcal{I}'$ and $\mathrm{cl}(\mathrm{cl}^{-1}(\mathcal{J})) = \mathcal{J}$. This bijection between the set of ideals of A containing $\mathcal{I}$ and the set of ideals of $A/\mathcal{I}$ respects inclusion.*

Note that this can be partly deduced from the next result which is useful by itself.

Proposition 1.15 *If $\mathcal{J}$ is an ideal of $A/\mathcal{I}$, then $\mathrm{cl}^{-1}(\mathcal{J})$ is the kernel of the composed ring homomorphism*

$$A \to A/\mathcal{I} \to (A/\mathcal{I})/\mathcal{J}.$$

This homomorphism factorizes through an isomorphism

$$A/\mathrm{cl}^{-1}(\mathcal{J}) \simeq (A/\mathcal{I})/\mathcal{J}.$$

This description of $\mathrm{cl}^{-1}(\mathcal{J})$ needs no comment. The factorization is a consequence of the factorization theorem.

Definition 1.16

(i) *An ideal generated by a finite number of elements is of finite type (or finitely generated).*
(ii) *An ideal generated by one element is principal.*

If $a_1, ..., a_n$ generate the ideal $\mathcal{J}$, we write $\mathcal{J} = (a_1, ..., a_n)$.

Theorem 1.17

(i) *All ideals in $\mathbb{Z}$ are principal.*

(ii) *If K is a field, all ideals in the polynomial ring (in one variable) $K[X]$ are principal.*

Proof Showing that a non-zero ideal $\mathcal{I}$ of $\mathbb{Z}$ is generated by the smallest positive integer of $\mathcal{I}$ is straightforward.

Following the same principle, let $\mathcal{I}$ be a non-zero ideal of $K[X]$. If $P \in \mathcal{I}$ is a non-zero polynomial such that $\deg(P) \leq \deg(Q)$ for all non-zero polynomials $Q \in \mathcal{I}$, showing that $\mathcal{I} = PK[X]$ is also straightforward. □

Definition 1.18 *Let A be a ring.*

(i) *If $a \in A$ is invertible, in other words if there exists $b \in A$ such that $ab = 1$, then a is a unit of A. One writes $b = a^{-1}$ and says that b is the inverse of a.*

(ii) *If $a \in A$ and $b \in B$ are elements such that $ab = 0$ and $b = 0$, we say that a is a zero divider.*

(iii) *If $a \in A$ is such that there exists an integer $n > 0$ such that $a^n = 0$, then a is nilpotent.*

Examples 1.19

1. The only units in $\mathbb{Z}$ are 1 and -1.
2. The units of $K[X]$ are the non-zero constants.
3. An element $\mathrm{cl}(m) \in \mathbb{Z}/n\mathbb{Z}$ is a unit if and only if m and n are relatively prime.
4. The ring $\mathbb{Z}/n\mathbb{Z}$ has no zero divisors if and only if n is prime.
5. The ring $\mathbb{Z}/n\mathbb{Z}$ has a non-zero nilpotent element if and only if n has a quadratic factor.
6. If $\mathcal{I} = (X^2 + Y^2, XY) \subset K[X,Y]$, then $\mathrm{cl}(X+Y), \mathrm{cl}(X)$ and $\mathrm{cl}(Y)$ are nilpotent elements of $K[X,Y]/\mathcal{I}$.

Definition 1.20

(i) *A non-zero ring without zero divisors is called a domain.*

(ii) *A non-zero ring without non-zero nilpotent elements is called a reduced ring.*

Definition 1.21 *A domain which is not a field and such that all its ideals are principal is a principal ideal ring.*

Hence our Theorem 1.17 can be stated in the following way.

Theorem 1.22 *The domains $\mathbb{Z}$ and $K[X]$ are principal ideal rings.*

1.2 Operations on ideals

Exercise 1.23 If $\mathcal{I}$ and $\mathcal{J}$ are ideals of a ring A, then $\mathcal{I} \cap \mathcal{J}$ is an ideal of A.

Note that if $\mathcal{I}$ and $\mathcal{J}$ are ideals of a ring A, then $\mathcal{I} \cup \mathcal{J}$ is not always an ideal of A.

Definition 1.24 *If $\mathcal{I}$ and $\mathcal{J}$ are ideals of a ring A, then*

$$\mathcal{I} + \mathcal{J} = \{a + b, \quad a \in \mathcal{I},\ b \in \mathcal{J}\}.$$

Note that $\mathcal{I} + \mathcal{J}$ is an ideal of A, obviously the smallest ideal containing $\mathcal{I}$ and $\mathcal{J}$.

Definition 1.25 *Let $\mathcal{I}_s$ be a family of ideals of A. We denote by $\sum_s \mathcal{I}_s$ the set formed by all finite sums $\sum_s a_s$, with $a_s \in \mathcal{I}_s$.*

We note once more that $\sum_s \mathcal{I}_s$ is an ideal of A, the smallest ideal containing $\mathcal{I}_s$ for all s.

Definition 1.26 *If $\mathcal{I}$ and $\mathcal{J}$ are ideals of A, the product $\mathcal{I}\mathcal{J}$ denotes the ideal generated by all ab with $a \in \mathcal{I}$ and $b \in \mathcal{J}$.*

Definition 1.27 *If $\mathcal{I}$ is an ideal of A and P a subset of A, we denote by $\mathcal{I} : P$ the set of all $a \in A$ such that $ax \in \mathcal{I}$ for all $x \in P$.*

If $P \not\subset I$, then $\mathcal{I} : P$ is a proper ideal of A. If $P \subset \mathcal{I}$, then $\mathcal{I} : P = A$.

Exercise 1.28 If $\mathcal{I}_i$, $i = 1, ..., n$, are ideals of A and P a subset of A, show that

$$(\bigcap_i \mathcal{I}_i) : P = \bigcap_i (\mathcal{I}_i : P).$$

Proposition 1.29 *If $f : A \to B$ is a ring homomorphism and $\mathcal{J}$ an ideal of B, then $f^{-1}(\mathcal{J})$ is an ideal of A (the contraction of $\mathcal{J}$ by f).*

Proof The kernel of the composition homomorphism $A \to B \to B/\mathcal{J}$ is $f^{-1}(\mathcal{J})$. □

Definition 1.30 *If $f : A \to B$ is a ring homomorphism and if $\mathcal{I}$ is an ideal of A, we denote by $f(\mathcal{I})B$ the ideal of B generated by the elements of $f(\mathcal{I})$.*

In other words, $f(\mathcal{I})B$ is the set consisting of all sums of elements of the form $f(a)b$ with $a \in \mathcal{I}$ and $b \in B$.

1.3 Prime ideals and maximal ideals

Definition 1.31 *An ideal $\mathcal{I}$ of A is prime if the quotient ring $A/\mathcal{I}$ is a domain.*

We note that a prime ideal has to be proper. The following result is obvious.

Proposition 1.32 *An ideal $\mathcal{I}$ is prime if and only if*

$$ab \in \mathcal{I} \quad \text{and} \quad a \notin \mathcal{I} \quad \Longrightarrow b \in \mathcal{I}.$$

Definition 1.33 *An ideal $\mathcal{I}$ of A is maximal if the quotient ring $A/\mathcal{I}$ is a field.*

Clearly, a maximal ideal is a prime ideal. The terminology is a bit unpleasant: obviously A is an absolute maximum in the set of all ideals, ordered by the inclusion. But the word maximal is justified by the following result:

Proposition 1.34 *An ideal $\mathcal{I}$ is maximal if and only if $\mathcal{I}$ is a maximal element of the set of all proper ideals, ordered by the inclusion.*

Proof A field is a ring whose only ideal is (0). Our proposition is an immediate consequence of Proposition 1.14. □

Exercises 1.35

1. Let k be a field and $(a_1, ..., a_n) \in k^n$. Show that the set of all polynomials $P \in k[X_1, ..., X_n]$, such that $P(a_1, ..., a_n) = 0$, is a maximal ideal of $k[X_1, ..., X_n]$ generated by $X_1 - a_1, ..., X_n - a_n$.
2. Show that all non-zero prime ideals of a principal ideal ring are maximal.

Proposition 1.36 *Let $\mathcal{P}$ be a prime ideal. If $\mathcal{I}_i$, with $i = 1, ..., n$, are ideals such that $\bigcap_1^n \mathcal{I}_i \subset \mathcal{P}$, there exists l such that $\mathcal{I}_l \subset \mathcal{P}$.*

Proof Assume not; then there exist $a_i \in \mathcal{I}_i$ and $a_i \notin \mathcal{P}$ for $i = 1, ..., n$. Since $\mathcal{P}$ is a prime ideal, this implies $\prod_1^n a_i \notin \mathcal{P}$. But $\prod_1^n a_i \in \bigcap_1^n \mathcal{I}_i$; this is a contradiction. □

Theorem 1.37 *(Avoiding lemma)*

Let $\mathcal{I}_1, .., \mathcal{I}_n$ be ideals of A such that at most two are not prime. If $\mathcal{J}$ is an ideal of A such that $\mathcal{J} \not\subset \mathcal{I}_m$ for $m = 1, ..., n$, then $\mathcal{J} \not\subset \bigcup_1^n \mathcal{I}_m$.

Proof We use induction on n. The result is clear for $n = 1$.

If $n > 1$, by the induction hypothesis, there exists, for all i, an element $a_i \in \mathcal{J}$, such that $a_i \notin \bigcup_{m \neq i} \mathcal{I}_m$. We can obviously assume $a_i \in \mathcal{I}_i$ for all i. Assume that $\mathcal{I}_1$ is prime if $n > 2$ and put $a = a_1 + \prod_{i>1} a_i$.

For $i > 1$ we have $a_1 \notin \mathcal{I}_i$ and $\prod_{i>1} a_i \in \mathcal{I}_i$. This shows $a \notin \mathcal{I}_i$ for $i > 1$. Since $\prod_{i>1} a_i \notin \mathcal{I}_1$ and $a_1 \in \mathcal{I}_1$, we have $a \notin \mathcal{I}_1$ and we are done. □

Note that we have proved in fact the following more general useful result.

Theorem 1.38 *Let $\mathcal{I}_1, .., \mathcal{I}_n$ be ideals of A such that at most two are not prime. If E is a subset of A, stable for addition and multiplication, such that $E \not\subset \mathcal{I}_m$ for $m = 1, ..., n$, then $E \not\subset \bigcup_1^n \mathcal{I}_m$.*

Proposition 1.39 *Let $\mathcal{I}$ be an ideal of A and let $\mathcal{J}$ be an ideal of A containing $\mathcal{I}$. Then $\mathcal{J}$ is a prime (resp. maximal) ideal of A if and only if $\mathcal{J}/\mathcal{I}$ is a prime (resp. maximal) ideal of $A/\mathcal{I}$.*

Proof The proposition is an immediate consequence of the ring isomorphism

$$A/\mathcal{J} \simeq (A/\mathcal{I})/(\mathcal{J}/\mathcal{I}).$$

□

Theorem 1.40 *A ring $A \neq 0$ has a maximal ideal.*

Let us first recall Zorn's lemma (or axiom):

Let E be a non-empty ordered set. If all totally ordered subsets of E are bounded above, E contains a maximal element.

Proof Consider $\mathcal{I}_i$, a totally ordered set of proper ideals of A. Define $\mathcal{I} = \bigcup_i \mathcal{I}_i$. We show that $\mathcal{I}$ is a proper ideal of A (obviously an upper bound for our totally ordered set).

If $a, b \in \mathcal{I}$ and $c \in A$, there exists $i \in E$ such that $a, b \in \mathcal{I}_i$. This implies $a + b \in \mathcal{I}_i \subset \mathcal{I}$ and $ac \in \mathcal{I}_i \subset \mathcal{I}$. Furthermore, since $1_A \notin \mathcal{I}_i$ for all i, it is clear that $1_A \notin \mathcal{I}$. □

Using Proposition 1.39, we get the following two corollaries.

Corollary 1.41 *Any proper ideal of a ring is contained in a maximal ideal.*

Corollary 1.42 *An element of a ring is invertible if and only if it is not contained in any maximal ideal of the ring.*

Definition 1.43

(i) *A ring with only one maximal ideal is local.*

(ii) *If A and B are local rings with respective maximal ideals $\mathcal{M}_A$ and $\mathcal{M}_B$, a homomorphism $f : A \to B$ such that $f(\mathcal{M}_A) \subset \mathcal{M}_B$ is called a local homomorphism of local rings.*

Exercises 1.44

1. Show that the ring $\mathbb{Z}_{(p)}$ (defined in Exercises 1.2) is local and that its maximal ideal is the set of all n/m with $n \in p\mathbb{Z}$ and $m \notin p\mathbb{Z}$.
2. Let K be a field and $(x_1, ..., x_n) \in K^n$. Show that the ring formed by all rational functions P/Q, with $P, Q \in K[X_1, ..., X_n]$ and such that $Q(x_1, ..., x_n) \neq 0$ is a local ring and that its maximal ideal is the set of all P/Q with $P(x_1, ..., x_n) = 0$ and $Q(x_1, ..., x_n) \neq 0$.

Definition 1.45 *The spectrum* Spec(A) *of a ring A is the set of all prime ideals of A.*

Proposition 1.46 *(Zariski topology)*
If, for each ideal $\mathcal{I}$ of A, we denote by $V(\mathcal{I}) \subset$ Spec(A) the set of all prime ideals $\mathcal{P}$ such that $\mathcal{I} \subset \mathcal{P}$, the subsets $V(\mathcal{I})$ of Spec(A) *are the closed sets of a topology on* Spec(A).

Proof If $\mathcal{I}_s$, with $s = 1, ..., n$, are ideals of A, then $\bigcup_1^n V(\mathcal{I}_s) = V(\bigcap_1^n \mathcal{I}_s)$.
If $\mathcal{I}_s$ is a family of ideals of A, then $\bigcap_s V(\mathcal{I}_s) = V(\sum_s \mathcal{I}_s)$. □

Note that by Corollary 1.41, a non-empty closed set of Spec(A) contains a maximal ideal.

Definition 1.47 *If $s \in A$, we denote by $D(s)$ the open set* Spec$(A) \setminus V(sA)$ *of* Spec(A).

We recall that a closed set of a topological space is irreducible if it is not the union of two strictly smaller closed subsets.

Proposition 1.48 *If $\mathcal{P}$ is a prime ideal of a ring A, the closed set $V(\mathcal{P}) \subset$* Spec(A) *is irreducible.*

Proof Let F_1 and F_2 be closed sets of Spec(A) such that $V(\mathcal{P}) = F_1 \bigcup F_2$. Then there exists i such that $\mathcal{P} \in F_i$. Consequently, we have $V(\mathcal{P}) = F_i$. □

As a special case, we get the following result.

Proposition 1.49 *Let A be a domain.*

(i) *The topological space* Spec(A) *is irreducible.*

(ii) *Any non-empty open subset of* Spec(A) *is dense in* Spec(A).

As we saw, the proof of this statement is straightforward. Its main consequence, which we will understand in due time, is that algebraic varieties are irreducible topological spaces for the Zariski topology.

1.4 Nilradicals and Jacobson radicals

Proposition 1.50 *The nilpotent elements of a ring A form an ideal of A.*

Proof If $a^n = 0$ and $b^m = 0$, then $(ca - db)^{n+m-1} = 0$. □

Corollary 1.51 *If $\mathcal{I}$ is an ideal of A, the set of all elements $a \in A$ having a power in $\mathcal{I}$ is an ideal of A.*

Proof Apply the proposition to the ring $A/\mathcal{I}$. □

Definition 1.52 *This ideal is the radical $\sqrt{\mathcal{I}}$ of $\mathcal{I}$. The radical $\sqrt{(0)}$ of (0) is the nilradical* Nil(A) *of A.*

Note that $\sqrt{\sqrt{\mathcal{I}}} = \sqrt{\mathcal{I}}$. As a consequence we see that if A is not the zero ring, then $A/\sqrt{(0)}$ is reduced.

Proposition 1.53 *A non-zero ring A is reduced if and only if* Nil$(A) = (0)$.

This is the definition of a reduced ring.

Theorem 1.54 *If A is not the zero ring, the nilradical* Nil(A) *is the intersection of all prime ideals of A.*

Proof Consider $a \in$ Nil(A) and $\mathcal{P}$ a prime ideal. There exists $n > 0$ such that $a^n = 0$, hence $a^n \in \mathcal{P}$ and $a \in \mathcal{P}$. This proves Nil$(A) \subset \mathcal{P}$.

Assume now $a \notin$ Nil(A) and let us show that there exists a prime ideal $\mathcal{P}$ such that $a \notin \mathcal{P}$. Consider the part S of A consisting of all positive powers of a. We have assumed that $0 \notin S$. We can therefore consider the non-empty set E of all ideals of A which do not intersect S. Let E' be a totally ordered subset of E. Clearly E' is bounded above, in E, by $\bigcup_{\mathcal{I} \in E'} \mathcal{I}$. By Zorn's lemma, E has a maximal element.

If $\mathcal{I}$ is a maximal element in E, let us show that $\mathcal{I}$ is a prime ideal.

Let $x, y \in A$ be such that $xy \in \mathcal{I}$. If $x \notin \mathcal{I}$ and $y \notin \mathcal{I}$, there are positive integers n and m such that $a^n \in \mathcal{I} + xA$ and $a^m \in \mathcal{I} + yA$. This implies

$$a^{n+m} \in \mathcal{I} + x\mathcal{I} + y\mathcal{I} + xyA \subset \mathcal{I},$$

hence a contradiction. □