
Lecture 2. Operations on ideals; maximal and prime ideals

We can define basic operations of addition and multiplication for ideals.

$$I + J = \{a + b \mid a \in I, b \in J\}$$

$$IJ = \left\{ \sum_{i=1}^t a_i b_i \mid a_i \in I, b_i \in J, t \in \mathbb{N} \right\}.$$

Multiplication of ideals is commutative: $IJ = JI$ and associative $I(JK) = (IJ)K$. We say that an ideal I divides an ideal K if there exists an ideal J such that $IJ = K$.

► The set of ideals of a ring itself is a multiplicative semigroup but is not a ring! There is no additive inverse.

► $I \cap J$ is also an ideal. In general, $IJ \subset I \cap J$.

◁ If $I = (m)$, $J = (n)$ in $\mathbb{Z}$, then $IJ = (mn)$, $I \cap J = (\text{lcm}(m, n))$ and $I + J = (\text{gcd}(m, n))$.

Proposition 2.1. *Suppose that the ideals I, J of a ring R are **coprime**, that is $I + J = R$, then $IJ = I \cap J$.*

Proof. $IJ \subset I \cap J$ by definition. To see the opposite inclusion, since $I + J = R$, we have $I \cap J = (I + J)(I \cap J) = I(I \cap J) + J(I \cap J) \subset IJ$. $\square$

Corollary 2.2. *Suppose I, J are coprime ideals in R , then $R/IJ \simeq R/I \times R/J$.*

Proof. It suffices to see that the natural injective map $\pi : R/IJ = R/(I \cap J) \rightarrow R/I \times R/J$ is surjective. Taking $x \in I$ and $y \in J$ such that $x + y = 1$, we have $bx + ay = a \in R/I$ and $bx + ay = b \in R/J$ for any $a, b \in R$ giving surjectivity. $\square$

By induction, we get the following theorem (known as the Sunzi remainder theorem when $R = \mathbb{Z}$).

Theorem 2.3. *Suppose $I_1, I_2, \dots, I_r$ are pairwise coprime ideals, that is, $I_i + I_j = R$ for $i \neq j$, then $I_1 I_2 \dots I_r = I_1 \cap I_2 \cap \dots \cap I_r$ and*

$$R/(I_1 \cap I_2 \cap \dots \cap I_r) \simeq R/I_1 \times R/I_2 \times \dots \times R/I_r.$$

Proof. We proceed by induction on r . The case $r = 2$ is already established. Let us put $J = I_2 \dots I_r$. We want to show that $I_1 + J = R$. Since $I_1 + I_i = R$ for all $i \geq 2$, we can find elements $a_i \in I_1$ and $b_i \in I_i$ such that $a_i + b_i = 1$. Then, we obtain

$$1 = \prod_{i=2}^r (a_i + b_i) = a + b_2 b_3 \dots b_r$$

where a is a sum of terms each of which contains at least one a_i as a factor. Therefore, $a \in I_1$. As $b_2 b_3 \dots b_r \in J$, we see that $I_1 + J = R$. Now, we can deduce that

$$R/I_1 J \simeq R/I_1 \times R/J$$

and the result follows by induction. $\square$

► There is also a quotient operation for ideals: $I : J := \{a \in R : aJ \subset I\}$, and the saturation $I : J^\infty := \{a \in R : aJ^n \subset I \text{ for some } n\}$.

◁ Check that $I : J$ and $I : J^\infty$ are ideals.

2.2.1 maximal, prime and $\sqrt{r}$ radical ideals

Every ideal contains the (0) ideal and is contained in the biggest ideal $(1) = R$.

A **maximal ideal** of a ring R is a proper ideal $\mathfrak{m}$ such that, for any ideal I , $\mathfrak{m} \subset I$ implies $\mathfrak{m} = I$ or $I = R$.

► An ideal $\mathfrak{m}$ is maximal if and only if $R/\mathfrak{m}$ is a field.

The next proposition is an application of Zorn's lemma which we recall first.

Zorn's lemma. Let $\mathcal{M}$ be a partially ordered set such that every totally ordered set $\mathcal{T} \subset \mathcal{M}$ has an upper bound, that is an element $b \in \mathcal{M}$ such that $t \leq b$ for all $t \in \mathcal{T}$. Then $\mathcal{M}$ has a maximal element $m \in \mathcal{M}$ such that if $x \in \mathcal{M}$ and $x \geq m$, then $x = m$.

Zorn's lemma is equivalent to the Axiom of Choice.

Proposition 2.4. *If I is a proper ideal, then there exists at least one maximal ideal containing I .*

Proof. Given a proper ideal I in R , let $\mathcal{M}$ be the set of proper ideals in R containing I . We can order elements of $\mathcal{M}$ by inclusion. Then Zorn's lemma can be applied to $\mathcal{M}$. Indeed, $I \in \mathcal{M}$ so $\mathcal{M}$ is non-empty, and if $\mathcal{T} \subset \mathcal{M}$ is a non-empty totally ordered subset, then the union of all the ideals belonging to $\mathcal{T}$ is an ideal of R containing I , and it is proper since it does not contain 1. Hence it belongs to $\mathcal{M}$ and is the least upper bound of $\mathcal{T}$. Thus, by Zorn's lemma, $\mathcal{M}$ has a maximal element, which is a maximal ideal of R containing I . $\square$

In fact, the assertion that every non-zero commutative unital ring has a maximal ideal is equivalent to the Axiom of Choice. I don't know how you feel about the Axiom of Choice. As one would expect, for the rings of main interest there are constructive ways of proving the above proposition (and so one doesn't really need to appeal to AC).

The main idea of algebraic geometry is that a commutative ring R is the space of functions on a space (an algebraic variety). The maximal ideals of R then correspond to geometric points of this space. For example, in the ring $R = \mathbb{C}[X, Y]$ the maximal ideals are $\mathfrak{m}_{a,b} = (X - a, Y - b)$, $(a, b) \in \mathbb{C}^2$. Indeed, this is the kernel of the evaluation homomorphism $\mathbb{C}[X, Y] \rightarrow \mathbb{C}$ sending a

polynomial f to its value $f(a, b)$. So, the points (a, b) of the space $\mathbb{C}^2$ correspond to the maximal ideals $\mathfrak{m}_{a,b}$ of the polynomial functions $\mathbb{C}[X, Y]$ on this space.

We will prove later in the course (“Nullstellensatz”) that there are no maximal ideals in the polynomial ring $\mathbb{C}[X, Y]$ other than $\mathfrak{m}_{a,b}$ with $(a, b) \in \mathbb{C}^2$.

If $f : R_1 \rightarrow R_2$ is a ring map and $\mathfrak{m}$ is a maximal ideal of R_2 then it need not be the case that $f^{-1}(\mathfrak{m})$ is a maximal ideal. For example, consider the inclusion $f : \mathbb{Z} \rightarrow \mathbb{Q}$ and observe that $f^{-1}((0)) = (0)$ is not maximal.

A proper ideal I in R is a **prime ideal** if whenever $xy \in I$, then $x \in I$ or $y \in I$.

► An ideal I is prime if and only if R/I is an integral domain.

In particular, a maximal ideal is prime.

Proposition 2.5. *If $f : R_1 \rightarrow R_2$ is a ring homomorphism and $\mathfrak{p} \subset R_2$ is a prime ideal, then $f^{-1}(\mathfrak{p})$ is a prime ideal.*

Proof. First, $f^{-1}(\mathfrak{p})$ is a proper ideal since $f(1) = 1 \notin \mathfrak{p}$. Suppose $xy \in f^{-1}(\mathfrak{p})$, then $f(xy) = f(x)f(y) \in \mathfrak{p}$. Hence, $f(x)$ or $f(y)$ is in $\mathfrak{p}$ since $\mathfrak{p}$ is prime. So, x or y is in $f^{-1}(\mathfrak{p})$. $\square$

► A positive integer n is a prime number if and only if (n) is a prime ideal in $\mathbb{Z}$.

Of course, since any maximal ideal is a prime ideal, the existence proof that we have given for maximal ideals implies that there are many prime ideals. However, we can be a bit more precise as in the following proposition.

A subset S of a ring is called a **multiplicative set** if

$$1 \in S, \text{ and } a, b \in S \implies ab \in S$$

(The difference from a subring is that we do not ask that S is closed under addition.)

Proposition 2.6. *(Krull’s lemma) Let R be a ring, $S \subset R$ a multiplicative set, and I an ideal of R disjoint from S . Then, there exists a prime ideal $\mathfrak{p}$ of R containing I and disjoint from S .*

Proof. Applying Zorn’s lemma, we can see as before that the set of ideals containing I and disjoint from S has a maximal element. We claim that this maximal element $\mathfrak{p}$ is a prime ideal. Suppose x and y are not in $\mathfrak{p}$. Then the ideals $\mathfrak{p} + (x)$ and $\mathfrak{p} + (y)$ both meet S , hence the ideal $(\mathfrak{p} + (x))(\mathfrak{p} + (y))$ also meets S . On the other hand, $(\mathfrak{p} + (x))(\mathfrak{p} + (y)) \subset \mathfrak{p} + (xy)$. Hence, $xy \notin \mathfrak{p}$. Thus, $\mathfrak{p}$ is prime. $\square$

A multiplicative set S is called **saturated** if it is closed under taking divisors: i.e., whenever $xy \in S$, the elements x and y are in S too.

< Show that S is a saturated multiplicative set if and only if the complement of S is a union of prime ideals (uses Zorn’s lemma).

Appendix: maximal ideals and the Axiom of Choice

We proved, using Zorn's lemma, that every proper ideal of a ring is contained in a maximal ideal; in particular, every non-zero ring has a maximal ideal. In this appendix we prove the converse mentioned in the text: the statement that every non-zero ring has a maximal ideal implies the Axiom of Choice. The result is due to Hodges³; we follow the recent exposition of Entin⁴, which keeps the argument within the language of this course. This appendix is not examinable.

We shall use the hypothesis in the following form.

■ **(MIT)** For every ring A and every multiplicative set $S \subset A$ with $0 \notin S$, there is an ideal of A which is maximal among the ideals of A disjoint from S .

► If every non-zero ring has a maximal ideal, then (MIT) holds. Indeed, in Lecture 18 we will construct from A and S a ring $S^{-1}A$, together with a homomorphism $\iota : A \rightarrow S^{-1}A$ such that $\iota(s)$ is a unit for every $s \in S$, and $S^{-1}A \neq 0$ precisely when $0 \notin S$. If M is a maximal ideal of $S^{-1}A$, then $\iota^{-1}(M)$ is disjoint from S , and it is maximal among such ideals: if $I \supsetneq \iota^{-1}(M)$, then the ideal generated by $\iota(I)$ strictly contains M (by Lemma 6.12(i)), hence contains 1, which forces $I \cap S \neq \emptyset$.

► The proof of Krull's lemma (Proposition 2.6) shows that an ideal which is maximal among the ideals disjoint from a multiplicative set is prime. We will use this.

Partially ordered sets. Let $(X, \leq)$ be a partially ordered set. An **upper bound** of a subset $Y \subset X$ is an element $x \in X$ with $y \leq x$ for all $y \in Y$. We say that Y is **compatible** if every finite subset of Y has an upper bound in X ; for example, every totally ordered subset is compatible. An element $x \in X$ is **maximal** if there is no $y \in X$ with $x < y$. Consider the following statement.

■ **(WZL)** Let X be a partially ordered set in which every compatible subset has an upper bound. Then X has a maximal element.

Since totally ordered subsets are compatible, Zorn's lemma implies (WZL). Conversely, (WZL) implies the Axiom of Choice, which is all we need.

Proposition. *(WZL) implies the Axiom of Choice.*

Proof. Let $(A_i)_{i \in I}$ be a family of non-empty sets; we must find a function f on I with $f(i) \in A_i$ for all i . Let X be the set of **partial choice functions**: functions f defined on a subset $\text{dom}(f) \subset I$ with $f(i) \in A_i$ for all $i \in \text{dom}(f)$. Order X by extension: $f \leq g$ if $\text{dom}(f) \subset \text{dom}(g)$ and g agrees with f on $\text{dom}(f)$.

Let $Y \subset X$ be compatible. For $f, g \in Y$ and $i \in \text{dom}(f) \cap \text{dom}(g)$, the pair $\{f, g\}$ has an upper bound h , so $f(i) = h(i) = g(i)$. Hence the functions in Y agree wherever two of them are

³W. Hodges, Krull implies Zorn, J. London Math. Soc. (2) 19 (1979), 285–287.

⁴A. Entin, Maximal ideals in commutative rings and the Axiom of Choice, arXiv:2404.18351 (2024).

defined, and their union is a partial choice function, which is an upper bound of Y . By (WZL), X has a maximal element f . If $\text{dom}(f) \neq I$, pick $i \in I \setminus \text{dom}(f)$ and $a \in A_i$; extending f by $f(i) = a$ gives an element strictly above f , a contradiction. So $\text{dom}(f) = I$ and f is a choice function. $\square$

Polynomials in partially ordered variables. Fix a partially ordered set X and a field k , and consider the polynomial ring $k[X]$ whose variables are the elements of X : its elements are finite k -linear combinations of **monomials**, that is, of finite products of variables (the empty product being 1). A monomial m **appears** in $f \in k[X]$ if its coefficient in f is non-zero, and a variable x **appears** in m if m is divisible by x .

Definition. Let $x \in X$ and $f \in k[X]$. We say that f is **dominated** by x , and write $f \leq x$, if every monomial appearing in f contains a variable y with $y \leq x$. A polynomial is **small** if it is dominated by some $x \in X$, and **big** otherwise. An ideal of $k[X]$ is **small** if all its elements are small, and a **maximal small ideal** is a small ideal not properly contained in any other small ideal.

Two observations follow at once from the definition: the polynomials dominated by a given x form an ideal, and if $f \leq x$ but $g \not\leq x$, then $f + g \not\leq x$. Note that 0 is small (it has no monomials) as soon as $X \neq \emptyset$, that a non-zero constant is big, and that a variable y is dominated by x if and only if $y \leq x$.

Lemma. The set S of big polynomials in $k[X]$ is a multiplicative set, and an ideal of $k[X]$ is small if and only if it is disjoint from S .

Proof. The second assertion is the definition. Clearly $1 \in S$. Let $f, g \in S$ and let $x \in X$. Write $f = f_1 + f_2$, where f_1 consists of the monomials of f that are dominated by x and f_2 of those that are not, and similarly $g = g_1 + g_2$. Since f and g are big, $f_2 \neq 0$ and $g_2 \neq 0$. No monomial of f_2 or of g_2 contains a variable $\leq x$, hence neither does any monomial of $f_2 g_2$, so $f_2 g_2 \not\leq x$. On the other hand $f_1 g_1 + f_1 g_2 + f_2 g_1 \leq x$ by the first observation above, so $fg = (f_1 g_1 + f_1 g_2 + f_2 g_1) + f_2 g_2 \not\leq x$ by the second. As x was arbitrary, fg is big. $\square$

Lemma. If $Y \subset X$ is compatible, then the ideal (Y) of $k[X]$ generated by Y is small.

Proof. An element of (Y) has the form $g = \sum_{i=1}^n g_i y_i$ with $y_i \in Y$ and $g_i \in k[X]$. Since Y is compatible, there is $x \in X$ with $y_i \leq x$ for all i , and then every monomial of g contains some $y_i \leq x$, so $g \leq x$. $\square$

Proposition. Let P be a maximal small ideal of $k[X]$ and let $Y = P \cap X$ be the set of variables lying in P . Then

- (i) $P = (Y)$;
- (ii) Y is compatible;
- (iii) Y is maximal compatible: if $Y \subset Y' \subset X$ and Y' is compatible, then $Y' = Y$.

Proof. By the first lemma and the remark on Krull's lemma above, P is a prime ideal.

(i) Clearly $(Y) \subset P$. Let $f \in P$ and let m be a monomial appearing in f ; we claim that some variable appearing in m lies in Y . Since f is small, $m \neq 1$, so we may pick a variable x appearing in m . Let $g \in P$ be arbitrary and let d be larger than the degree of g . The polynomial $h = x^d f + g$ lies in P , hence is dominated by some $y \in X$. Every monomial of $x^d f$ has degree at least d in x , while every monomial of g has degree less than d in x , so no cancellation occurs in the sum: the monomials of g and the monomial $x^d m$ all appear in h . Therefore $g \leq y$ and $x^d m \leq y$; the latter means that $m \leq y$, as m and $x^d m$ contain the same variables. It follows that $g + qm \leq y$ for every $q \in k[X]$. Since $g \in P$ was arbitrary, every element of the ideal $P + (m)$ is small, and the maximality of P gives $m \in P$. As P is prime, some variable appearing in m lies in P , that is, in Y . This proves the claim, and the claim says precisely that $f \in (Y)$.

(ii) Let $x_1, \dots, x_n \in Y$ be distinct. Then $x_1 + \dots + x_n \in P$ is small, so it is dominated by some $x \in X$; as its monomials are the x_i , this means $x_i \leq x$ for all i . Thus every finite subset of Y has an upper bound.

(iii) By the second lemma, (Y') is a small ideal, and it contains $(Y) = P$. By maximality $(Y') = P$, hence $Y' = (Y') \cap X = P \cap X = Y$. $\square$

Theorem. (*Hodges*) Assume (MIT). Then the Axiom of Choice holds.

Proof. By the first proposition it suffices to prove (WZL). So let X be a partially ordered set in which every compatible subset has an upper bound. The empty subset is compatible, so it has an upper bound and $X \neq \emptyset$. Let S be the set of big polynomials in $k[X]$; it is a multiplicative set with $0 \notin S$. By (MIT), there is an ideal P of $k[X]$ which is maximal among the ideals disjoint from S , that is, a maximal small ideal. By the second proposition, $Y = P \cap X$ is a maximal compatible subset of X . By hypothesis Y has an upper bound x . We claim that x is a maximal element of X . Otherwise $x < y$ for some $y \in X$. Then $y \notin Y$ (as $y \leq x$ would give $y < y$), and $Y \cup \{x, y\}$ is compatible, since y is an upper bound of all of it. This contradicts the maximality of Y . $\square$

► The proof shows a little more: the maximal small ideals of $k[X]$ correspond exactly to the maximal compatible subsets of X , so (MIT) for the single ring $S^{-1}k[X]$ already produces a maximal element of X .