

ALGEBRA HANDOUT 2: IDEALS AND QUOTIENTS

PETE L. CLARK

1. IDEALS IN COMMUTATIVE RINGS

In this section all groups and rings will be commutative.

1.1. Basic definitions and examples. Let R be a (commutative!) ring. An **ideal** of R is a subset I of R satisfying:

- (IR1) I is a subgroup of the additive group of R .
- (IR2) For any $r \in R$ and any $i \in I$, $ri \in I$.

We often employ notation like $rI = \{ri \mid i \in I\}$ and then (IR2) can be stated more succinctly as: for all $r \in R$, $rI \subset I$. In other words, an ideal is a subset of a ring R which is a subgroup under addition (in particular it contains 0 so is nonempty) and is not only closed under multiplication but satisfies the *stronger* property that it “absorbs” all elements of the ring under multiplication.

Remark (Ideals versus subrings): It is worthwhile to compare these two notions; they are related, but with subtle and important differences. Both an ideal I and a subring S of a ring R are subsets of R which are subgroups under addition and are stable under multiplication. However, each has an additional property: for an ideal it is the *absorption* property (IR2). For instance, the integers \mathbb{Z} are a subring of the rational numbers \mathbb{Q} , but are clearly not an ideal, since $\frac{1}{2} \cdot 1 = \frac{1}{2}$, which is not an integer. On the other hand a subring has a property that an ideal usually lacks, namely it must contain the unity 1 of R . For instance, the subset $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ is an ideal of \mathbb{Z} but is not a subring.

Example 1 (trivial ideals): Any ring R (which is not the zero ring!) contains at least two ideals: the ideal $\{0\}$, and the ideal R itself. These are however not very interesting examples, and often need to be ignored in a discussion. (The convention that “ideal” should stand for “non-zero ideal” whenever convenient is a fairly common and useful one in the subject.) An ideal I is said to be **proper** if it is not R , and again most interesting statements about ideals should really be applied to proper ideals. Note well that an ideal is proper iff it does not contain the unity 1. Indeed, an ideal lacking 1 is certainly proper, and conversely, if $1 \in I$ and $r \in R$, then $r \cdot 1 = r$ is in I .

Proposition 1. *The following are equivalent for a nonzero commutative ring R :*

- a) R has only the trivial ideals $\{0\}$ and R .
- b) R is a field.

Thanks to Chris Pryby for pointing out a typo in these notes.

Proof: b) \implies a): Suppose I is a nonzero ideal of a field R , so I contains some $0 \neq a$. Then since a is a field, a^{-1} exists and $1 = a^{-1}a \in R \cdot I \subset I$, so I contains 1 and is hence all of R .

a) \implies b): Suppose R is not a field; then some nonzero element a does not have an inverse. Then the set $aR = \{ar \mid r \in R\}$ is a proper, nonzero ideal.

The preceding argument shows a general construction of ideals: for any element a of R , the set of elements $\{ra \mid r \in R\}$ is an ideal of R . (Just to check: $r_1a + r_2a = (r_1 + r_2)a$, $-ra = (-r)a$ and $r'(ra) = (r'r)a$.) We denote such ideals as either Ra or (a) ; they are simple and easy to understand and are called **principal ideals** and a is called a *generator*.

Proposition 2. (*To contain is to divide*) Let a and b be elements of R . The following are equivalent:

a) $(a) \supset (b)$.

b) $a \mid b$; i.e., $b = ac$ for some c in R .

Proof: For ideals in \mathbb{Z} , this is exercise 2.4. The proof in the general case is the same.

Proposition 3. Let a and b be elements of an integral domain R . The following are equivalent:

a) $(a) = (b)$.

b) $a = bu$ for some unit $u \in R^\times$.

Proof: Since $(a) \supset (b)$, $b = c_1a$ for some $c_1 \in R$. Since $(b) \supset (a)$, $a = c_2b$ for some $c_2 \in R$. Combining this information we get $b = c_1c_2b$. If $b = 0$, then also $a = 0$, a trivial case; otherwise, we can cancel b to get $c_1c_2 = 1$, meaning that c_1 and c_2 are units, so $a = c_2b$ shows what we want.

Pairs a and b satisfying the equivalent conditions of the preceding proposition are said to be **associates**; “ x is associate to y ” is an equivalence relation. For example, the associates of n in \mathbb{Z} are $\pm n$.

The notion of generators for ideals can be generalized: for any a_1, \dots, a_n , there is an ideal, denoted (a_1, \dots, a_n) , and defined as the set of all elements of the form $a_1r_1 + \dots + a_nr_n$ as r_1, \dots, r_n range over all elements of R . This is called the ideal *generated by* a_1, \dots, a_n , and it is not hard to see that any ideal I which contains the elements a_1, \dots, a_n must contain the ideal (a_1, \dots, a_n) .

Of course, an ideal which is generated by n elements may also be generated by fewer elements. For instance, we proved that every ideal in the integers was generated by a single element, the gcd: $(a_1, \dots, a_n) = (\gcd(a_1, \dots, a_n))$.¹ This leads us to the following important

Definition: A ring R is called *principal* if every ideal is principal, and a principal integral domain is called a **principal ideal domain** (PID)

¹Because of this identity, it is common to write (a_1, \dots, a_n) as an abbreviation for the gcd. We will preserve the more careful notation at least for a while longer.

Example 2: Trivially, a field is a principal ideal domain: the only ideals of a field are (0) and $(1) = F$, and these are principal.

Example 3: The ring $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ – i.e., the set of pairs (a, b) with $a, b \in \mathbb{Z}/2\mathbb{Z}$ and componentwise addition and multiplication – is not an integral domain: $(1, 0) \cdot (0, 1) = 0$. More generally, one can check that the product $R_1 \times R_2$ of two nonzero principal ideal domains is a principal ring which is not a domain if neither R_1 nor R_2 is the zero ring.²

Example 4: Let $R = \mathbb{Z}[T]$, and consider the ideal $(2, T)$: it consists of all polynomials of the form $2P(T) + TQ(T)$. Is this ideal principal? If so, there would exist a single magic polynomial $M(T)$ such that $2 = p_1(T) \cdot M(T)$ and $T = p_2(T) \cdot M(T)$. The first equation implies $M(T) = 1$ or 2 . The equation $T = 2 \cdot p_2(T)$ being impossible (the leading coefficient of $p_2(T)$ would have to be $\frac{1}{2}$, but that is not an element of R), we must have $M(T) = 1$. But then the ideal $(2, T)$ would be the unit ideal and this isn't true either: we cannot have

$$2P(T) + TQ(T) = 1 :$$

plugging $T = 0$ gives $2P(0) = 1$, which is impossible.

Example 5: As we showed in class (handout on the Gaussian integers), the integral domain $\mathbb{Z}[\sqrt{-5}]$ is not a PID.

Example 5 is a deeper example of a nonprincipal domain than Example 4, for reasons that we will not be able to fully go into. Roughly speaking, the ring $\mathbb{Z}[T]$ is “too big” to be a PID. Somewhat more precisely, in terms of further properties of ideals to be discussed presently, one can define the **(Krull) dimension** of a commutative ring. A domain is a field iff it has Krull dimension zero; any PID has dimension 1, and the dimension of $R[T]$ is one more than the dimension of R . From these claims we deduce that the dimension of $\mathbb{Z}[T]$ is 2 and that it is therefore not a PID. However, $\mathbb{Z}[\sqrt{-5}]$ is a one dimensional domain which is not a PID, and this is much more interesting.

1.2. Prime and maximal ideals. A proper ideal I in a ring is **prime** if whenever $xy \in I$, $x \in I$ or $y \in I$. A proper ideal is **maximal** if it is not strictly contained in any larger proper ideal.

This is quite a presumptuous definition: it says that the “true nature of primality” is a property of ideals, not of elements. Grudgingly, we admit that it gives the correct definition for ideals in \mathbb{Z} : an ideal I is prime iff it is generated by a prime number (this follows from Euclid's Lemma and its converse, Exercise 2.3). However, in more general rings, the principal ideal generated by an irreducible element may *not* be a prime ideal: this occurs in $\mathbb{Z}[\sqrt{-5}]$, where, recall, we have inequivalent irreducible factorizations:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Here $2|6$ but 2 does not divide $1 \pm \sqrt{-5}$, because $\frac{1}{2} \pm \frac{1}{2}\sqrt{5}$ is just not an element of $\mathbb{Z}[\sqrt{-5}]$. Thus the ideal (2) in $\mathbb{Z}[\sqrt{-5}]$ is *not* a prime ideal, despite the fact that 2

²While typing these notes, it occurred to me to wonder whether every finite ring is principal.

cannot be factored further.

Leaving aside these subtle and interesting issues, we record a few more routine observations. The proofs of the next two propositions merely involving matching up the definitions, so are left as informal exercises for the interested reader.

Proposition 4. *A ring is an integral domain iff the zero ideal is prime.*

Proposition 5. *A ring is a field iff the zero ideal is maximal.*

The following is a little less routine:

Proposition 6. *In a principal ideal domain, every nonzero prime ideal is maximal.*

Proof: Suppose (a) is a prime ideal which is not maximal: then we have a proper containment of ideals $(a) \subsetneq (b)$, with (b) a proper ideal. By Proposition 2, this means that $a = bc$ for some $c \in R$. Since (a) is prime, we get that either $b \in (a)$ or $c \in (a)$. The former implies that $(a) = (b)$, contradicting the strictness of the containment. So $c \in (a)$; say $c = da$. Then $a = b(da) = bda$. Since $a \neq 0$, we can cancel, getting $bd = 1$. Thus b is a unit, so (b) is not a proper ideal, a contradiction.

Example 6: In $\mathbb{Z}[T]$, the ideal (T) is prime: a polynomial is divisible by T iff its constant term is zero. And if $P_1(T)$ has constant term c_1 and $P_2(T)$ has constant term c_2 , then $P_1(T)P_2(T)$ has constant term c_1c_2 , so if $P_1(T)P_2(T)$ has constant term zero, so does at least one of P_1 and P_2 . On the other hand it is not maximal, since it is strictly contained in the proper ideal $(2, T)$.

Definition: A **finite ascending chain** of ideals in a ring R is a sequence

$$I_0 \subsetneq I_1 \subsetneq \dots \subsetneq I_n$$

of ideals, in which each ideal is properly contained in the next. We will say that the **length** of the chain is n , so that a single ideal I forms a chain of length 0.

Definition: The **Krull dimension** of a ring R is the largest possible length of an ascending chain of **prime** ideals, or ∞ there exist such chains of length n for every integer n .

The interested reader can now verify some of the claims made in the last section: e.g. fields are characterized among integral domains by having dimension 0, and that PID's have length 1 (all maximal chains are of the form $0 \subsetneq P$). If $I_0 \subsetneq I_1 \subsetneq \dots \subsetneq I_n$ is a chain of prime ideals of R , then

$$I_0 \subsetneq I_1 \dots \subsetneq I_n \subsetneq \langle I_n, T \rangle$$

is a chain of length $n + 1$ in the polynomial ring $R[T]$: here $\langle I_n, T \rangle$ is the ideal of all elements of the form $P(T)i_n + Q(T)T$, with $i_n \in I_n$ and $P(T), Q(T) \in R[T]$. This shows that the dimension of $R[T]$ is at least one more than the dimension of R . We omit the proof of the other direction (and we will not need it).

2. QUOTIENT RINGS

Probably the most important single use of ideals is the quotient construction: if I is an ideal in a (still assumed commutative) ring R , then we can form a ring R/I

endowed with a canonical homomorphism $R \rightarrow R/I$, as follows:

The elements of R/I are the cosets $r + I$ of the subgroup I of R . The addition and multiplication laws are derived from those on R :

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2 + I).$$

$$(r_1 + I) \cdot (r_2 + I) = (r_1 r_2 + I).$$

One must check that these definitions actually make sense (“are well-defined”): namely, that the sum and product of cosets does not depend upon the choice of representative we chose. After all, $r_1 + I$ is the same coset as $r_1 + i_1 + I$, for any $i_1 \in I$. Now we just check that the properties of I are exactly such as to ensure that the final answer tolerates such ambiguity: suppose we chose $r_1 + i_1$ and $r_2 + i_2$ instead. Then we would have defined the sum to be

$$r_1 + i_1 + r_2 + i_2 + I = r_1 + r_2 + (i_1 + i_2 + I).$$

But since $i_1, i_2 \in I$, so is $i_1 + i_2$, which means that $i_1 + i_2 + I = I$, so it’s okay: we get the same coset no matter what i_1 and i_2 we pick. And similarly for multiplication:

$$(r_1 + i_1 + I)(r_2 + i_2 + I) = (r_1 + i_1)(r_2 + i_2) + I = r_1 r_2 + r_1 i_2 + r_2 i_1 + i_1 i_2.$$

But again by the absorption property (IR2) of ideals, $r_1 i_2, r_2 i_1$, and $i_1 i_2$ are all elements of I , and hence so is their sum. (This shows why a mere subring wouldn’t do!) Thus R/I is indeed a ring. Moreover, the map $R \rightarrow R/I$ is just $r \mapsto r + I$. It is essentially tautological that it is a homomorphism of rings.

When two elements r_1 and r_2 determine the same coset $r_1 + I = r_2 + I$, their images in R/I are equal (and conversely). In this situation, it is useful to say that r_1 and r_2 are equal *modulo* I .

Example 7: Consider the ideal (n) in \mathbb{Z} , where n is some positive integer. Then a choice of representative for each coset $\mathbb{Z} + (n)$ is obtained by taking $0, 1, \dots, n - 1$. In other words, for any two distinct integers $0 \leq i, j < n$, $i - j$ is not a multiple of n , so $i + (n)$ and $j + (n)$ are distinct cosets. Moreover, for any larger integer k , the coset $k + (n)$ will be equal to a unique coset $i + (n)$, where i is the remainder upon dividing k by n .

The ring $\mathbb{Z}/(n)$ is nothing else than the finite ring we denoted Z_n , and the “naive” recipe we gave for the addition and multiplication operations on Z_n – i.e., do addition and multiplication as usual in \mathbb{Z} and then take the remainder modulo n in the sense of the Division Theorem – is made rigorous by the quotient construction: it is a systematization of the process of “throwing away multiples of n .”

Example 8: Let us look at the quotient $\mathbb{Z}[i]/(2)$: can we identify this ring? The first thought is that it is just $\mathbb{Z}/2\mathbb{Z}$, but this is wrong: the elements $a + bi$ which are congruent to zero modulo (2) are those of the form $2(c + di) = 2c + 2di$: i.e., both the real and imaginary parts must be even. From this it follows that, at least additively, $\mathbb{Z}[i]/(2)$ is the “square” of $\mathbb{Z}/(2)$: a set of coset representatives is given by $0, 1, i, 1 + i$. In plainer terms, no two of these elements differ by a Gaussian integer $c + di$ with c and d both even, and given any Gaussian integer $a + bi$, we can subtract appropriate even numbers A from a and B from b to get $c + di$ with

$0 \leq c, d \leq i$. In fact the same argument shows that, as commutative groups, $\mathbb{Z}[i]/(n)$ is isomorphic to $\mathbb{Z}/(n) \times \mathbb{Z}/(n)$.

However, there is also the matter of the multiplicative structure to consider: is it perhaps $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$ also as a ring?

The answer is no. Indeed, notice that $(1+i)^2 = (1+i)(1+i) = 1+2i+i^2 = 2i \equiv 0 \pmod{2\mathbb{Z}[i]}$, so that the representative $r = 1+i$ in the quotient is a nonzero element whose square is zero. That is, it is a nilpotent element, so that $\mathbb{Z}[i]/(2)$ is a nonreduced ring, whereas $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has zero divisors but no nilpotent elements. So the ring structure is in fact a bit unfamiliar. Perhaps the best way to package it is by noticing that $\mathbb{Z}[i]/(2)$ contains $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ as a subring, and is generated by adjoining to $\mathbb{Z}/2\mathbb{Z}$ the single element $r = 1+i$. Thus one can show that it is isomorphic to the ring $\mathbb{Z}/2\mathbb{Z}[X]/(X^2)$, or, if you like, the ring $\mathbb{Z}[X]/(2, X^2)$.

It is natural to wonder what the ring structure on the n^2 element quotient $\mathbb{Z}[i]/(n)$ is. There is some real number theory involved here: you might enjoy playing around with small primes p to see what happens. You will see that the case $p = 2$ is quite exceptional: for all other primes, the quotient ring $\mathbb{Z}[i]/(p)$ is reduced, and is an integral domain iff $p \equiv 3 \pmod{4}$. When $p \equiv 1 \pmod{4}$, the ring structure really is $\mathbb{Z}/(p) \times \mathbb{Z}/(p)$, whereas when $p \equiv 3 \pmod{4}$ we get a finite integral domain – hence a field! – of order p^2 . We will come back to this example later.

Many properties of ideals I are equivalent to certain properties of the quotient ring R/I . Here are two very important examples:

Proposition 7. *Let I be an ideal in a ring R .*

- a) I is prime iff R/I is an integral domain.*
- b) I is maximal iff R/I is a field.*

Proof: The ideal I is prime if, whenever $xy \in I$, either $x \in I$ or $y \in I$. Now an element x lies in I iff its image in R/I is zero, so an ideal I is prime if whenever a product of two elements $x+I$ and $y+I$ is zero in R/I , at least one of $x+I$ and $y+I$ is zero. This is the definition of an integral domain!

If R/I is a field, then whenever $x \notin I$, there exists an element $y \in R$ such that $(x+I)(y+I) = (xy+I) = (1+I)$, i.e., $xy - 1 = i \in I$. If I is not maximal, there exists some element $x \in R \setminus I$ and a proper ideal J containing I and x . But $1 = xy - i$, so any ideal which contains both I and x also contains xy and $-i$, hence contains 1, so is not proper. Similarly, if I is maximal and x is any element of $R \setminus I$, then the set $I_x = \{i + rx \mid i \in I, r \in R\}$ is an ideal containing I and x , hence I_x strictly contains I so must contain 1. That is, $1 = i + yx$ for some $i \in I, y \in R$, and this means that $(x+I)(y+I) = 1+I$, so that $x+I$ is invertible in R/I .

Example 9: Let $R = F[X, Y]$ for any field F . Then $R/(X) \cong F[Y]$: we are considering polynomials $P(X, Y)$ modulo multiples of X , and this amounts to evaluating $X = 0$ and considering the corresponding polynomials $P(0, Y)$, which form the ring $F[Y]$. Since the quotient ring $F[Y]$ is an integral domain, (X) is a prime ideal. Since it is not a field, (X) is not maximal. Therefore R is not a PID. Note that we showed this without exhibiting any particular nonprincipal ideal. Tracking through the preceding proofs, we see that there must be a nonprincipal ideal which contains (X) ; can you find one?