Due date: 22.10.2019

1 Ideals

This section is intended for those who have not encountered ideals in ring theory before. You should not expect any revelations here, we will cover basic material only.

1.1 Ideals in commutative rings

Before we jump right to the definition, let us first consider an example. Recall that the set of integers with the usual addition and multiplication has the structure of a ring. And a very pleasant kind of ring at that: among many other properties—such as the absence of nasty zero divisors—$(\mathbb{Z}, +, \cdot)$ is a commutative ring, hence we do not need to worry about the order of the operands during multiplication or addition. The set of even numbers is a special subset within this ring:

1. The sum of two even numbers is again an even number. So the even numbers are closed under addition.
2. An even number times any integer is an even number. Thus, even numbers remain even when multiplied by elements of the enclosing ring.

These are the characteristic properties of ideals.

Definition 1 (Ideal)
Let $(R, +, \cdot)$ be a commutative ring. An ideal[1] *I is a nonempty subset of R that is closed under addition and stable under multiplication by elements of the enclosing ring. More formally, a subset $I \subseteq R$, $I \neq \emptyset$, is an ideal if both of the following conditions are satisfied.*

1. $\forall i, j \in I : i + j \in I$
2. $\forall r \in R \, \forall i \in I : r \cdot i \in I.$ ∎

Ideals contained in the ring of integers will not be of much interest to us. Instead, we shall focus our attention on polynomial ideals. The set of even numbers is an ideal with an implicit description. Sometimes, however, it is necessary to speak about an ideal that is generated by some ring elements (similar to the linear span of a set of vectors).

[1] The definition of ideal given here is not the most general one. In order to define ideals in arbitrary rings, one has to specify from which side the ring elements are multiplied in the second condition. We speak of a *left ideal* if the set is stable under multiplication by ring elements from the left and analogously for *right ideals*. If such multiplication is allowed from both sides we speak of a *two-sided* ideal. All of these notions coincide while multiplication is commutative. Consequently, we call such objects merely *ideals* when working in commutative rings.

Definition 2 (Generated ideal)
Let $(R, +, \cdot)$ be a commutative ring. Given a finite number of ring elements $g_1, \dots, g_n \in R$, we define the set

$$\langle g_1, \dots, g_n \rangle := \left\{ \sum_{i=1}^{n} r_i \cdot g_i \;\middle|\; r_i \in R \right\}.$$

This set is called the ideal generated by $g_1, \dots, g_n$ *and the elements $g_1, \dots, g_n$ are known as the* generators *of the ideal.* ■

Exercise
Prove that the set $\langle g_1, \dots, g_n \rangle$ from Definition 2 is indeed an ideal, i.e. it is closed under addition and stable under multiplication by elements of the enclosing ring. Furthermore, show that this set is the smallest ideal that contains all generators.

Ideals generated by a family of polynomials have a very nice interpretation. Assume we have a system of equations

$$\begin{aligned} f_1(x_1, \dots, x_n) &= 0 \\ f_2(x_1, \dots, x_n) &= 0 \\ &\vdots \\ f_m(x_1, \dots, x_n) &= 0, \end{aligned} \tag{1}$$

where $f_i(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ are polynomials. In order to solve this system one has to perform some kind of elimination. For example, given the system

$$\begin{aligned} x - 1 + z^2 &= 0 \\ y - 1 + z &= 0 \end{aligned}$$

we can eliminate the variable z by multiplying the second equation with $y - 1 - z$ followed by adding the result to the first equation. This yields the equation

$$(y - 1 - z) \cdot (y - 1 + z) + (x - 1 + z^2) = y^2 - x - 2y = 0.$$

If we allow that equations can be added and multiplied by arbitrary polynomials (not just scalars as in linear algebra), then the set

$$\langle f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n) \rangle \subseteq K[x_1, \dots, x_n]$$

can be thought of as the set of all polynomial equations which can be derived from the original system (1). There also is a close connection between vanishing sets (the set of roots) of polynomials and ideals in polynomial rings. Consider the curve in Figure 1 which is defined as the set

$$\left\{ (x, y) \subseteq \mathbb{R}^2 \mid f(x, y) = 0 \right\},$$

where $f(x, y) = \left(x^2 + y^2\right)^3 - 4x^2y^2 \in \mathbb{R}[x, y]$. Sets which can be defined as the zero locus of a polynomial (or a family of polynomials) are called *affine algebraic sets*. They are the central objects of study in classical algebraic geometry.

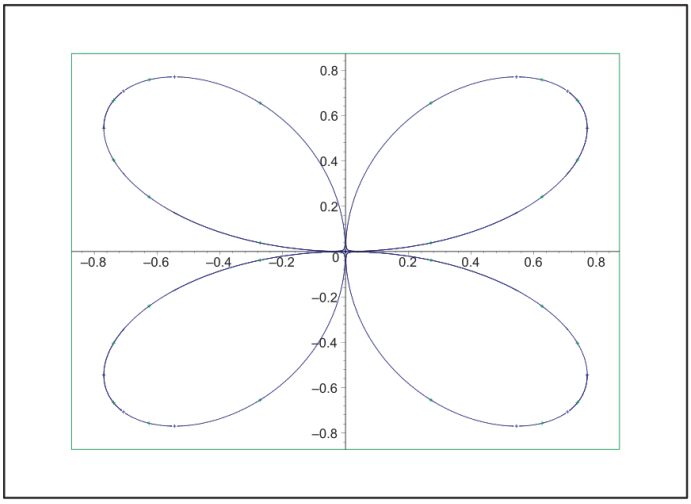

Figure 1: Real part of the curve cut out by the polynomial $f(x,y) = \left(x^2+y^2\right)^3 - 4x^2y^2$.

Exercise
Let $V \subseteq K^n$ be an affine algebraic set, where K is a field. Let us define

$$\mathbf{I}(V) := \{f(x_1,\dots,x_n) \in K[x_1,\dots,x_n] \mid \forall (v_1,\dots,v_n) \in V : f(v_1,\dots,v_n) = 0\},$$

which is the set of all polynomial that vanish at all points in V. Show that $\mathbf{I}(V)$ is an ideal.

A famous theorem in algebraic geometry, called *Hilbert's Nullstellensatz*, states that affine algebraic sets are in one-to-one correspondence with certain ideals in polynomial rings over an appropriate field. We will not give details here, since the theorem would require some background in commutative algebra and algebraic geometry. The message to take away is that there is a tight link between geometric objects (curves or surfaces defined by polynomial equations) and algebraic structures (polynomial ideals). Such a link allows us to tackle problems from two sides: the geometric side is convenient for visualising objects and to gain some intuition, whereas the algebraic counterpart is well suited for manipulating such objects on computers.

1.2 Principal ideal domains (PIDs)

We have seen how to produce an ideal from a number of generating elements, similar to the linear span of a set of vectors in linear algebra. What about the opposite direction? Given an ideal I, is it possible to find a (finite) number of elements which generate I? This

question should again remind you of some concept[2] from linear algebra. The answer to the aforementioned question is: it is difficult and depends heavily on the enclosing ring. Since it was promised at the beginning of the section that we consider only basic material, i.e. non-difficult material, we shall restrict to the easy cases. Ideals which are generated by a single element have a special name.

Definition 3 (Principal ideal)
Let I be an ideal in a commutative ring R. We call I principal *if it can be generated by a single element. In other words, I is called a* principal ideal *if there exists an element $g \in I$ such that $\langle g \rangle = I$.* ■

It is clear that every ideal that is generated by a single element is principal, but what about the ideal

$$\langle 6, 9, 33 \rangle \subseteq \mathbb{Z}.$$

This ideal is generated by three numbers and does not seem to be principal at first sight. Yet it turns out that the very same ideal can be generated by a single element, namely

$$\langle 3 \rangle = \langle 6, 9, 33 \rangle .$$

Do you see why? Recall that in linear algebra, we can show that two sets of vectors generate the same vector space if we can write each vector in one set as a linear combination of the vectors in the other set and vice versa. The same holds for ideals: To show that two sets of generators produce the same ideal one has to show that each of the generators can be obtained from the other generating set. For the example above:

1. $\langle 3 \rangle \subseteq \langle 6, 9, 33 \rangle$ since $3 = (-1) \cdot 6 + 1 \cdot 9 + 0 \cdot 33$.
2. $\langle 6, 9, 33 \rangle \subseteq \langle 3 \rangle$ since $6 = 2 \cdot 3$, $9 = 3 \cdot 3$ and $33 = 11 \cdot 3$.

Which proves that $\langle 3 \rangle = \langle 6, 9, 33 \rangle$ since they are contained in each other. In general, given an integer ideal $I = \langle g_1, \dots, g_n \rangle \subseteq \mathbb{Z}$ generated by finitely many integers, then I is also generated by the GCD of those generators, i.e.

$$I = \langle gcd\,(g_1, \dots, g_n) \rangle .$$

Exercise
Let $2\mathbb{Z} = \{2 \cdot i \mid i \in \mathbb{Z}\}$ be the ideal of even numbers. Is this ideal principal and if yes, by what element is it generated?

There are certain domains (i.e. integral domains) where every ideal can be generated by a single element. This adds yet another name to the long list of algebraic structures we have seen so far.

Definition 4 (Principal ideal domain (PID))
A principal ideal domain *is an integral domain in which every ideal is principal.* ■

[2] Bases of vectors spaces is the answer, of course.

Let us conclude this section by providing two examples of PIDs (we assume the usual addition and multiplication for both of them):

1. $\mathbb{Z}$: The ring of integers is a PID.
2. $K[x]$: The polynomial ring in one variable over a field K is a PID.

2 Exercises

GCD Greatest common divisor
ED Euclidean domain
PID Principal ideal domain

Exercise 1
Apply the extended Euclidean algorithm to compute the GCD and the Bézout cofactors of the polynomials

$$a(x) = x^3 + 3x^2 + 2x + 1 \quad \text{and} \quad b(x) = x^2 + x + 1$$

over the field of rational numbers by hand. Alternatively, you may implement the algorithm `GCD_EUCLID` in a computer algebra system and print the individual steps of the algorithm with input $a(x), b(x)$.

Exercise 2
Let us extend the definition of GCD to finitely many polynomials (cf. Definition 2.1.1 in the lecture notes): A *greatest common divisor* of a finite number of polynomials $f_1(x), \dots, f_n(x) \in K[x]$, where K is a field and $n \geq 2$, is a polynomial $g(x) \in K[x]$ with the following properties:

1. $g(x)$ divides all polynomials $f_1(x), \dots, f_n(x)$.
2. If $h(x)$ is another polynomial which divides all $f_1(x), \dots, f_n(x)$, then $h(x)$ divides $g(x)$.

When $g(x)$ satisfies these properties, we write $g(x) = gcd(f_1(x), \dots, f_n(x))$.

The GCD of a finite number of polynomials exists and is unique up to multiplication by nonzero constants in K. Now prove the following items:

1. The GCD generates the ideal spanned by the f_i, i.e.

$$\langle gcd(f_1(x), \dots, f_n(x)) \rangle = \langle f_1(x), \dots, f_n(x) \rangle .$$

2. For $n > 2$ the identity

$$gcd(f_1(x), f_2(x), \dots, f_n(x)) = gcd(f_1(x), gcd(f_2(x), \dots, f_n(x)))$$

holds. This shows that we can compute the GCD of finitely many polynomials with the (two-input) algorithm `GCD_EUCLID`.

Hint: If $g_2(x) = gcd(f_2(x), \dots, f_n(x))$, show that $\langle f_1(x), g_2(x) \rangle = \langle f_1(x), \dots, f_n(x) \rangle$ and use the uniqueness property.

Exercise 3
It was mentioned at the end of the introduction that the polynomial ring in one variable over a field K is a PID. This exercise demonstrates that this is no longer true in the multivariate case. Consider the ideal

$$I = \langle x, y \rangle \subseteq K[x, y].$$

Show that the ideal I is not principal.

Hint (elementary approach): If I would be principal, show that a generator $g(x, y)$ would have to satisfy $deg_x(g(x, y)) = deg_y(g(x, y)) = 1$, where deg_x and deg_y denote the degree of a polynomial in the variable x and y, respectively. Use this to derive a contradiction.

Exercise 4
Which of the following domains (with the usual addition and multiplication) are EDs and which are not? Justify your answer.

1. $\mathbb{Z}$ with degree function $deg(i) = |i|$
2. $\mathbb{Q}$ with degree function $deg(q) = |q|$
3. $\mathbb{Z}[i]$, i.e. the Gaussian integers, with degree function $|z|^2$
4. $K[x]$, where K is a field, with degree function $deg(f) = degree(f)$, i.e. the degree of the polynomial f
5. $K[x, y]$, where K is a field, with degree function $deg(f) = degree(f)$, i.e. the total degree of the polynomial f