MIT 6.972 Algebraic techniques and semidefinite optimization	February 16, 2006

Lecture 4

Lecturer: Pablo A. Parrilo *Scribe: Pablo A. Parrilo*

In this lecture we will review some basic elements of abstract algebra. We also introduce and begin studying the main objects of our considerations, multivariate polynomials.

1 Review: groups, rings, fields

We present here standard background material on abstract algebra. Most of the definitions are from [Lan71, CLO97, DF91, BCR98].

Definition 1 *A* group *consists of a set G and a binary operation "$\cdot$" defined on G, for which the following conditions are satisfied:*

1. *Associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all $a, b, c \in G$.*
2. *Identity: There exist $1 \in G$ such that $a \cdot 1 = 1 \cdot a = a$, for all $a \in G$.*
3. *Inverse: Given $a \in G$, there exists $b \in G$ such that $a \cdot b = b \cdot a = 1$.*

For example, the integers $\mathbb{Z}$ form a group under addition, but not under multiplication. Another example is the set $GL(n, \mathbb{R})$ of real nonsingular $n \times n$ matrices, under matrix multiplication.

If we drop the condition on the existence of an inverse, we obtain a *monoid*. Note that a monoid always has at least one element, the identity. As an example, given a set S, then the set of all strings of elements of S is a monoid, where the monoid operation is string concatenation and the identity is the empty string λ. Another example is given by $\mathbb{N}_0$, with the operation being addition (in this case, the identity is the zero). Monoids are also known as *semigroups with identity*.

In a group we only have one binary operation ("multiplication"). We will introduce another operation ("addition"), and study the structure that results from their interaction.

Definition 2 *A* commutative ring *(with identity) consists of a set k and two binary operations "$\cdot$" and "$+$", defined on k, for which the following conditions are satisfied:*

1. *Associative: $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all $a, b, c \in k$.*
2. *Commutative: $a + b = b + a$ and $a \cdot b = b \cdot a$, for all $a, b \in k$.*
3. *Distributive: $a \cdot (b + c) = a \cdot b + a \cdot c$, for all $a, b, c \in k$.*
4. *Identities: There exist $0, 1 \in k$ such that $a + 0 = a \cdot 1 = a$, for all $a \in k$.*
5. *Additive inverse: Given $a \in k$, there exists $b \in k$ such that $a + b = 0$.*

A simple example of a ring are the integers $\mathbb{Z}$ under the usual operations. After formally introducing polynomials, we will see a few more examples of rings.

If we add a requirement for the existence of multiplicative inverses, we obtain *fields*.

Definition 3 *A* field *consists of a set k and two binary operations "$\cdot$" and "$+$", defined on k, for which the following conditions are satisfied:*

1. *Associative: $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all $a, b, c \in k$.*
2. *Commutative: $a + b = b + a$ and $a \cdot b = b \cdot a$, for all $a, b \in k$.*
3. *Distributive: $a \cdot (b + c) = a \cdot b + a \cdot c$, for all $a, b, c \in k$.*

4. *Identities: There exist $0, 1 \in k$, where $0 \neq 1$, such that $a + 0 = a \cdot 1 = a$, for all $a \in k$.*

5. *Additive inverse: Given $a \in k$, there exists $b \in k$ such that $a + b = 0$.*

6. *Multiplicative inverse: Given $a \in k, a \neq 0$, there exists $c \in k$ such that $a \cdot c = 1$.*

Any field is obviously a commutative ring. Some commonly used fields are the rationals $\mathbb{Q}$, the reals $\mathbb{R}$ and the complex numbers $\mathbb{C}$. There are also Galois or finite fields (the set k has a finite number of elements), such as $\mathbb{Z}_p$, the set of integers modulo p, where p is a prime. Another important field is given by $k(x_1, \ldots, x_n)$, the set of *rational functions* with coefficients in the field k, with the natural operations.

2 Polynomials and ideals

Consider a given field k, and let $x_1, \ldots, x_n$ be indeterminates. We can then define *polynomials*.

Definition 4 *A* polynomial *f in $x_1, \ldots, x_n$ with coefficients in a field k is a finite linear combination of monomials:*

$$f = \sum_{\alpha} c_\alpha x^\alpha = \sum_{\alpha} c_\alpha x_1^{\alpha_1} \ldots x_n^{\alpha_n}, \qquad c_\alpha \in k, \tag{1}$$

where the sum is over a finite number of n-tuples $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\alpha_i \in \mathbb{N}_0$. The set of all polynomials in $x_1, \ldots, x_n$ with coefficients in k is denoted $k[x_1, \ldots, x_n]$.

It follows from the previous definitions that $k[x_1, \ldots, x_n]$, i.e., the set of polynomials in n variables with coefficients in k, is a commutative ring with identity. We also notice that it is possible (and sometimes, convenient) to define polynomials where the coefficients belong to a ring with identity, not necessarily to a field.

Definition 5 *A* form *is a polynomial where all the monomials have the same degree $d := \sum_i \alpha_i$. In this case, the polynomial is* homogeneous *of degree d, since it satisfies $f(\lambda x_1, \ldots, \lambda x_n) = \lambda^d f(x_1, \ldots, x_n)$.*

A commutative ring is called an *integral domain* if it has no *zero divisors*, i.e. $a \neq 0, b \neq 0 \Rightarrow a \cdot b \neq 0$. Every field is also an integral domain (why?). Two examples of rings that are not integral domains are the set of matrices $\mathbb{R}^{n \times n}$, and the set of integers modulo n, when n is a composite number (with the usual operations). If k is an integral domain, then so is $k[x_1, \ldots, x_n]$.

Remark 6 *Another important example of a ring (in this case, non-commutative) appears in systems and control theory, through the ring $\mathcal{M}(s)$ of stable proper rational functions. This is the set of matrices (of fixed dimension) whose entries are rational functions of s (i.e., in the field $\mathbb{C}(s)$), are bounded at infinity, and have all poles in the strict left-half plane. In this algebraic setting (usually called "coprime factorization approach"), the question of finding a stabilizing controller is exactly equivalent to the solvability of a Diophantine equation $ax + by = 1$.*

2.1 Algebraically closed and formally real fields

A very important property of a univariate polynomial p is the existence of a *root*, i.e., an element x_0 for which $p(x_0) = 0$. Depending on the solvability of these equations, we can characterize a particular nice class of fields.

Definition 7 *A field k is* algebraically closed *if every nonconstant polynomial in $k[x]$ has a root in k.*

If a field is algebraically closed, then it has an infinite number of elements (why?). What can we say about the most usual fields, $\mathbb{C}$ and $\mathbb{R}$? The Fundamental Theorem of Algebra ("every univariate polynomial has at least one complex root") shows that $\mathbb{C}$ is an algebraically closed field.

However, this is clearly *not* the case of $\mathbb{R}$, since for instance the polynomial x^2+1 does not have any real root. The lack of algebraic closure of $\mathbb{R}$ is one of the main sources of complications when dealing with systems of polynomial equations and inequalities. To deal with the case when the base field is not algebraically closed, the *Artin-Schreier* theory of *formally real fields* was introduced.

The starting point is one of the intrinsic properties of $\mathbb{R}$:

$$\sum_{i=1}^{n} x_i^2 = 0 \quad \Longrightarrow \quad x_1 = \ldots = x_n = 0. \tag{2}$$

A field will be called *formally real* if it satisfies the above condition (clearly, $\mathbb{R}$ and $\mathbb{Q}$ are formally real, but $\mathbb{C}$ is not). As we can see from the definition, the theory of formally real fields has very strong connections with sums of squares, a notion that will reappear in several forms later in the course. For example, an alternative (but equivalent) statement of (2) is to say that a field is formally real if and only if the element -1 is not a sum of squares.

A related important notion is that of an *ordered* field:

Definition 8 *A field k is said to be* ordered *if a relation $>$ is defined on k, that satisfies*

1. *If $a, b \in k$, then either $a > b$ or $a = b$ or $b > a$.*
2. *If $a > b$, $c \in k$, $c > 0$ then $ac > bc$.*
3. *If $a > b$, $c \in k$, then $a + c > b + c$.*

A crucial result relating these two notions is the following:

Lemma 9 *A field can be ordered if and only if it is formally real.*

For a field to be ordered (or equivalently, formally real), it necessarily must have an infinite number of elements. This is somewhat unfortunate, since this rules out several modular methods for dealing with real solutions to polynomial inequalities.

2.2 Ideals

We consider next *ideals*, which are subrings with an "absorbent" property:

Definition 10 *Let R be a commutative ring. A subset $I \subset R$ is an* ideal *if it satisfies:*

1. *$0 \in I$.*
2. *If $a, b \in I$, then $a + b \in I$.*
3. *If $a \in I$ and $b \in R$, then $a \cdot b \in I$.*

A simple example of an ideal is the set of even integers, considered as a subset of the integer ring $\mathbb{Z}$. Also, notice that if the ideal I contains the multiplicative identity 1, then $I = R$.

To introduce another important example of ideals, we need to define the concept of an algebraic variety as the zero set of a set of polynomial equations:

Definition 11 *Let k be a field, and let $f_1, \ldots, f_s$ be polynomials in $k[x_1, \ldots, x_n]$. Let the set $\mathbf{V}$ be*

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n : f_i(a_1, \ldots, a_n) = 0 \qquad \forall 1 \le i \le s\}.$$

We call $\mathbf{V}(f_1, \ldots, f_s)$ the affine variety *defined by $f_1, \ldots, f_s$.*

Then, the set of polynomials that vanish in a given variety, i.e.,

$$\mathbf{I}(V) = \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \qquad \forall (a_1, \ldots, a_n) \in V\},$$

is an ideal, called the *ideal of* V.

By Hilbert's Basis Theorem [CLO97], $k[x_1, \ldots, x_n]$ is a *Noetherian* ring, i.e., every ideal $I \subset k[x_1, \ldots, x_n]$ is finitely generated. In other words, there always exists a finite set $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ such that for every $f \in I$, we can find $g_i \in k[x_1, \ldots, x_n]$ that verify $f = \sum_{i=1}^{s} g_i f_i$.

We also define the *radical* of an ideal:

Definition 12 *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. The* radical *of I, denoted $\sqrt{I}$, is the set*

$$\{f \mid f^k \in I \text{ for some integer } k \geq 1\}.$$

It is clear that $I \subset \sqrt{I}$, and it can be shown that $\sqrt{I}$ is also a polynomial ideal. A very important result, that we will see later in some detail, is the following:

Theorem 13 (Hilbert's Nullstellensatz) *If I is a polynomial ideal, then $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$.*

2.3 Associative algebras

Another important notion, that we will encounter at least twice later in the course, is that of an *associative algebra*.

Definition 14 *An* associative algebra *$\mathcal{A}$ over $\mathbb{C}$ is a vector space with a $\mathbb{C}$-bilinear operation $\cdot : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ that satisfies*

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z, \qquad \forall x, y, z \in \mathcal{A}.$$

In general, associative algebras do not need to be commutative (i.e., $x \cdot y = y \cdot x$). However, that is an important special case, with many interesting properties. We list below several examples of finite dimensional associative algebras.

- Full matrix algebra $\mathbb{C}^{n \times n}$, standard product.
- The subalgebra of square matrices with equal row and column sums.
- The n-dimensional algebra generated by a single $n \times n$ matrix.
- The group algebra: formal $\mathbb{C}$-linear combination of group elements.
- Polynomial multiplication modulo a zero dimensional ideal.
- The Bose-Mesner algebra of an association scheme.

We will discuss the last three in more detail later in the course.

3 Questions about polynomials

There are many natural questions that we may want to answer about polynomials, even in the univariate case. Among them, we mention:

- When does a univariate polynomial have *only* real roots?
- What conditions must it satisfy for *all* roots to be real?
- When does a polynomial satisfy $p(x) \geq 0$ for all x?

We will answer many of these next week.

References

[BCR98] J. Bochnak, M. Coste, and M-F. Roy. *Real Algebraic Geometry*. Springer, 1998.

[CLO97] D. A. Cox, J. B. Little, and D. O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer, 1997.

[DF91] D. S. Dummit and R. M. Foote. *Abstract algebra*. Prentice Hall Inc., Englewood Cliffs, NJ, 1991.

[Lan71] S. Lang. *Algebra*. Addison-Wesley, 1971.