A FIRST COURSE

IN

ABSTRACT ALGEBRA

A FIRST COURSE

IN

ABSTRACT ALGEBRA

MAT3004 Notebook

Dr. Guang Rao

The Chinese University of Hongkong, Shenzhen

香港中文大學(深圳)
The Chinese University of Hong Kong, Shenzhen

Contents

Acknowledgments

This book is from the MAT3004 in fall semester, 2018.

CUHK(SZ)

Notations and Conventions

$\mathbb{R}^n$	n-dimensional real space
$\mathbb{C}^n$	n-dimensional complex space
$\mathbb{R}^{m\times n}$	set of all $m \times n$ real-valued matrices
$\mathbb{C}^{m\times n}$	set of all $m \times n$ complex-valued matrices
x_i	ith entry of column vector $\boldsymbol{x}$
a_{ij}	(i,j)th entry of matrix $\boldsymbol{A}$
$\boldsymbol{a}_i$	ith column of matrix $\boldsymbol{A}$
$\boldsymbol{a}_i^{\mathrm{T}}$	ith row of matrix $\boldsymbol{A}$
$\mathbb{S}^n$	set of all $n \times n$ real symmetric matrices, i.e., $\boldsymbol{A} \in \mathbb{R}^{n\times n}$ and $a_{ij} = a_{ji}$ for all i,j
$\mathbb{H}^n$	set of all $n \times n$ complex Hermitian matrices, i.e., $\boldsymbol{A} \in \mathbb{C}^{n\times n}$ and $\bar{a}_{ij} = a_{ji}$ for all i,j
$\boldsymbol{A}^{\mathrm{T}}$	transpose of $\boldsymbol{A}$, i.e, $\boldsymbol{B} = \boldsymbol{A}^{\mathrm{T}}$ means $b_{ji} = a_{ij}$ for all i,j
$\boldsymbol{A}^{\mathrm{H}}$	Hermitian transpose of $\boldsymbol{A}$, i.e, $\boldsymbol{B} = \boldsymbol{A}^{\mathrm{H}}$ means $b_{ji} = \bar{a}_{ij}$ for all i,j
$\mathrm{trace}(\boldsymbol{A})$	sum of diagonal entries of square matrix $\boldsymbol{A}$
$\mathbf{1}$	A vector with all 1 entries
$\mathbf{0}$	either a vector of all zeros, or a matrix of all zeros
$\boldsymbol{e}_i$	a unit vector with the nonzero element at the ith entry
$\mathcal{C}(\boldsymbol{A})$	the column space of $\boldsymbol{A}$
$\mathcal{R}(\boldsymbol{A})$	the row space of $\boldsymbol{A}$
$\mathcal{N}(\boldsymbol{A})$	the null space of $\boldsymbol{A}$
$\mathrm{Proj}_{\mathcal{M}}(\boldsymbol{A})$	the projection of $\boldsymbol{A}$ onto the set $\mathcal{M}$

8.3. Friday

8.3.1. Polynomials

Definition 8.13 [polynomial] Let k be a field, and $f = \sum_{i=0}^{n} c_i x^i$ be a polynomial in $k[x]$. An element $a \in k$ is a root of f if

$$f(a) = \sum_{i=0}^{n} c_i a^i = 0$$

in k.

question: what is $k[x]$?

Corollary 8.2 For all $f \in k[x]$, $a \in k$, then there exists $q \in k[x]$ such that

$$f = q(x-a) + f(a)$$

Proof. By division theorem, there exists $q, r \in k[x]$ such that

$$f = q \cdot (x-a) + r, \quad \deg r < \deg(x-a) = 1$$

which implies r is a constant. Evaluate both sides for $x = a$, we have

$$f(a) = r.$$

■

Proposition 8.18 — **root theorem.** Let k be a field, f a polynomial is $k[x]$. Then $a \in k$ is a root of f iff $(x-a)$ divides f in $k[x]$.

Proof. For forward direction, there exists $q \in k[x]$ such that

$$f = q(x-a) + f(a) = q(x-a) \implies (x-a) | f$$

For the reverse direction, if $f = q(x-a)$ for some $q \in k[x]$, then $f(a) = q(a)(a-a) = 0$, i.e., a is a root of f. ∎

Theorem 8.6 Let k be a field, f a nonzero polynomial in $k[x]$

1. If f has some degree n, then it has at most n roots in k
2. If f has degree n and $a_1, \dots, a_n \in k$ are distinct roots of f, then

$$f = c\prod_{i=1}^{n}(x - a_i)$$

for some $c \in k$.

Proof. 1. We show the first part by induction. Suppose it holds for all nonzero polynomails with degree strictly less than n, and $\deg f = n$. If f has no roots in k, the proof is complete, otherwise suppose a root $a \in k$. There exists $q \in k[x]$ such that

$$f = q(x - a)$$

For the any other root $b \in k$, we have

$$0 = q(b)(b - a)$$

Since k is a firld, it has no zero divisors, which implies $q(b) = 0$, since $b - a \neq 0$. Thus b is a root of q. Since $\deg q < n$, by induction we imply q has at most $n - 1$ roots, i.e., f has at most $n - 1$ roots that are different from a.

2. If $n = 1$, then $f = c_0 + c_1 x$ for some $c_i \in k$ with $c_1 \neq 0$, which implies

$$0 = f(a_1) = c_0 + c_1 a_1 \implies c_0 = -c_1 a_1 \implies f = -c_1 a_1 + c_1 x = c_1(x - a_1)$$

Suppose $n > 1$, and the claim holds for all $n' \in \mathbb{N}$ such that $n' < n$. By previuos claim, there exists $q \in k[x]$ such that

$$f = q(x - a_n)$$

Since $\deg q = n-1$, and for $1 \le i < n$, we have

$$0 = f(a_i) = q(a_i)(a_i - a_n) \implies q(a_i = 0),$$

which implies $a_1, \ldots, a_{n-1}$ are $n-1$ distinct roots of q as well. Thus there exists $c \in k$ s.t.

$$q = c(x-a_1)\cdots(x-a_{n-1}),$$

which follows that

$$f = q(x-a_n) = c(x-a_1)\cdots(x-a_n)$$

■

Corollary 8.3 Let k be a field. Let f, g be nonzero polynomails in $k[x]$. Let $n = \max\{\deg f, \deg g\}$. If $f(a) = g(a)$ for $n+1$ distinct $a \in k$, then $f = g$.

Proof. Let $h = f - g$, then $\deg h \le n$. There are $n+1$ distinct elements $a \in k$ s.t. $h(a) = 0$. If $h \neq 0$, then it is a nonzero polynomial of degree $\le n$ which has $n+1$ distinct roots, which is a constraction. $h = 0$ implies $f = g$. ■

Definition 8.14 A polynomail in $k[x]$ is called a **monic polynomial** if its leading coefficient is 1.

Theorem 8.7 Let k be a field, then the ring $k[x]$ is a PID.

Corollary 8.4 Let k be a field, and f, g be nonzero polynomials in $k[x]$. There exists a unique monic polynomial $d \in k[x]$ with the following properties:

1. $(f, g) = (d)$
2. d divides both f and g, i.e., there exists $a, b \in k[x]$ s.t. $f = ad, g = bd$
3. There are polynomials $p, q \in k[x]$ such that $d = pf + qg$
4. If $h \in k[x]$ is a divisor of f, g, then h divides d.

This $d \in k[x]$ is called the **greatest common divisor** (GCD) of f and g. We say f and g are **relatively prime** if their GCD is 1.

Proof. By the PID theorem, there exists $d = \sum_{n=0}^{\infty} a_i x^i \in k[x]$ such that $(d) = (f,g)$. Replacing d with $a_n^{-1}d$, we assume d is a monic polynomial. It remains to show that d is unique.

Suppose $(d) = (d')$, there exists nonzero $p,q \in k[x]$ such that

$$d' = pd, \quad d = qd'$$

which follows that

$$\deg d' = \deg d + \deg p, \quad \deg d = \deg q + \deg d' = \deg q + \deg d + \deg p,$$

i.e., $\deg p = \deg q = 0$. Thus $\deg d = \deg d'$. Comparing the leading coefficients of d' and pd, we have $p = 1$, i.e., $d = d'$.

The remaining part follows similarly. ■

Definition 8.15 [Irreducible] Let R be a commutative ring. A non-zero element $p \in R$ which is not a unit is said to be **irreducible** if $p = ab$ implies that either a or b is a unit.

■ **Example 8.10** The set of irreducible elements in the ring $\mathbb{Z}$ is

$$\{\pm p \mid p \text{ is a prime number}\}$$

Let k be a field.

Proposition 8.19 A polynomial $f \in k[x]$ is a unit iff it is a **nonzero** constant polynomial.

Proposition 8.20 A nonzero nonconstant polynoimial $p \in k[x]$ is **irreducible** iff there is no $f,g \in k[x]$ with $\deg f, \deg g < \deg p$, such that $fg = p$.

Proof. 1. Suppose p is irreducible, and $p = fg$ for some $f,g \in k[x]$ such that $\deg f, \deg g <$

$\deg p$. Then $p = fg$ implies that $\deg f, \deg g$ are both positive. By previous lemma, both f, g are non-units, which is a contradiction.

2. Conversely, suppose p is a nonzero non-unit in $k[x]$, which is not equal to fg for $\forall f, g \in k[x]$ with $\deg f, \deg g < \deg p$. Then $p = ab$ for $a, b \in k[x]$ implies that either a or b must have the same degree as p, and the otehr factor must be a nonzero constant, i.e., a unit in $k[x]$. Thus p is irreducible.

■

Proposition 8.21 — **Euclid's Lemma.** Let k be a field. Let f, g be polynomials in $k[x]$. Let p be an irreducible polynomial in $k[x]$. If $p | fg$ in $k[x]$, then $p | f$ or $p | g$.

Proof. Suppose p not divides f, then any **common divisor** of p and f must have degree strictly less than $\deg p$. Since p is irreducible, this implies that any common divisor of p and f is a nonzero constant. Thus the GCD of p and f is 1. There exists $a, b \in k[x]$ such that

$$ap + bf = 1 \implies apg + bfg = g$$

Since p divides the LHS, it also divides the RHS. ■

Proposition 8.22 If $f, g \in k[x]$ are relatively prime, and both divide $h \in k[x]$, then $fg | h$.

question

Theorem 8.8 — **Unique Factorization.** Let k be a field. Every non-constant polynomial $f \in k[x]$ may be written as

$$f = cp_1 \cdots p_n$$

where c is a non-zero constant, and each p_i is a monic irreducible polynomials in $k[x]$. The factorization is **unique** up to the ordering of the factors.

Proof. Similar to the proof of unique factorization for $\mathbb{Z}$ ■

Theorem 8.9 Let k be a field, p be a polynomial in $k[x]$. The following statements are equivalent:

1. $k[x]/(p)$ is a field
2. $k[x]/(p)$ is an integral domain
3. p is irreducible in $k[x]$.

Proof.

1. (2) implies (3): If p is not irreducible, then there exists $f,g \in k[x]$ with degree strictly less than that of p, such that $p = fg$.
   It's clear that p does not divide f or g in $k[x]$. The equivalence classes $\bar{f}$ and $\bar{g}$ of f and g, respectively, modulo (p) is not equal to zero in $k[x]/(p)$. (question) On the other hand, $\bar{f} \cdot \bar{g} = \bar{fg} = \bar{p} = 0$ in $k[x]/(p)$, which implies that $k[x]/(p)$ is not an integral domain, which is a contradction.
2. (3) implies (1): By definiton, the multiplicative identity 1 of a field is different from addictive identity 0. We first check that the equivalence lcass $1 \in k[x]$ in $k[x]/(p)$ is not zero. Since p is irreducible, we have $\deg p > 0$, and $1 \notin (p)$. Therefore $1 + (p) \neq 0 + (p)$ in $k[x]/(p)$.
   Next, we need to show the existence of multiplicative inverse of any nonzero element in $k[x]/(p)$. Given any $f \in k[x]$ whose equivalence $\bar{f}$ modulo (p) is nonzero in $k[x]/(p)$, we want to constracut $\bar{f}^{-1}$. Since $\bar{f} \neq 0$ in $k[x]/(p)$, we have $f - 0 \notin (p)$, i.e., p does not divide f. Since p is irreducible, we have $gcd(p,f) = 1$. There exists $g,h \in k[x]$ such that $fg + hp = 1$. Thus $\bar{f}^{-1} = \bar{g}$. This is becasue $fg - 1 = hp$ implies $fg - 1 \in (p)$, i.e., $\bar{f}\bar{g} = \bar{fg} = 1$ in $k[x]/(p)$.

■

8.3.2. Polynomials over $\mathbb{Z}$ and $\mathbb{Q}$

Theorem 8.10 Let $f = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial in $\mathbb{Q}[x]$, with $a_i \in \mathbb{Z}$. Every rational root r of f in $\mathbb{Q}$ has the form $r = b/c$ $(b,c \in \mathbb{Z})$, where $b|a_0$ and $c|a_n$

Proof. Let $r = b/c$ be a rational root of f, where b,c are relatively prime integers. We have

$$0 = \sum_{i=1}^{n} a_i (b/c)^i$$

Multiplying both sides above equation by c^n, we have

$$0 = a_0 c^n + a_1 c^{n-1} b + \cdots + a_n b^n$$

or equivalently,

$$a_0 c^n = -(a_1 c^{n-1} + \cdots + a_n b^n)$$

Since b divides the RHS, and b, c are relatively prime, b must divide a_0. Similarly,

$$a_n b^n = -(a_0 c^n + \cdots + a_{n-1} c b^{n-1})$$

It is clear that c divides a_n. ■

Definition 8.16 A polynomial $f \in \mathbb{Z}[x]$ is said to be **primitive** if the gcd of its coefficients is 1.

R Note that if f is monic, i.e., its leading coefficient is 1, then it is primitive. If d is the gcd of the coefficients of f, then $\frac{1}{d} f$ is a primitive polynomial in $\mathbb{Z}[x]$.

Theorem 8.11 — Gauss's Lemma. If f, g are both primitive, then fg is primitive.

Proof. Write $f = \sum_{k=0}^{m} a_k x^k$ and $g = \sum_{k=0}^{n} b_k x^k$, then $fg = \sum_{k=0}^{m+n} c_k x^k$, where

$$c_k = \sum_{i+j=k} a_i b_j.$$

Assume that fg is not primitive, then there exists a prime p such that p divides c_k for $k = 0, 1, \ldots, m+n$. Since f is primitive, there exists smallest u s.t. a_u is not dividible by p; similarly, a smallest v s.t. b_v is not divisible by p. We have

$$c_{u+v} = \left(\sum_{i+j=u+v, (i,j) \neq (u,v)} a_i b_j \right) + a_u b_v,$$

which implies that

$$a_u b_v = c_{u+v} - \left(\sum_{i+j=u+v, i<u} a_i b_j \right) - \left(\sum_{i+j=u+v, i>u} a_i b_j \right)$$

By the minimum conditons on u and v, each term on the RHS of the above equation is divisible by p. Thus p divides a_u and b_v, which implies that p divides either a_u or b_v, which is a contradiction. ■

Proposition 8.23 Every nonzero $f \in \mathbb{Q}[x]$ has a unique factorization:

$$f = c(f) f_0,$$

where $c(f)$ is a positive rational number, and f_0 is a primitive polynomial in $\mathbb{Z}[x]$.

Definition 8.17 The rational number $c(f)$ is called the **content** of f. ■