LINEAR ALGEBRA II

Bo Yu（于波）Dalian University of Technology

线性代数II（B.YU）

Ch. XI Polynomials and Primary Decomposition

- **Theorem 1.3.** *Let f be a polynomial with complex coefficients, leading coefficient* 1, *and* $\deg f = n \geqq 1$. *Then there exist complex numbers* $\alpha_1, \ldots, \alpha_n$ *such that*

$$f(t) = (t - \alpha_1) \cdots (t - \alpha_n).$$

The numbers $\alpha_1, \ldots, \alpha_n$ *are uniquely determined up to a permutation. Every root* α *of* f *is equal to some* α_i, *and conversely.*

- $$f(t) = (t - \alpha_1)^{m_1} \cdots (t - \alpha_r)^{m_r}$$ $\alpha_i \neq \alpha_j \quad (i \neq j)$

- m_i : the multiplicity of α_i

-

§1. THE EUCLIDEAN ALGORITHM

- **Theorem 1.1.** *Let f, g be polynomials over the field K, i.e. polynomials in $K[t]$, and assume* $\deg g \geqq 0$. *Then there exist polynomials q, r in $K[t]$ such that*

$$f(t) = q(t)g(t) + r(t),$$

and $\deg r < \deg g$. *The polynomials q, r are uniquely determined by these conditions.*

§1. THE EUCLIDEAN ALGORITHM

§1. THE EUCLIDEAN ALGORITHM

- Long division（长除，division with remainder（带余除法））
- Example：$f(t) = 3t^4 - 4t^3 + 5t - 1,\ g(t) = t^2 - t + 1.$

- **Corollary 1.2.** *Let f be a non-zero polynomial in $K[t]$. Let $\alpha \in K$ be such that $f(\alpha) = 0$. Then there exists a polynomial $q(t)$ in $K[t]$ such that*

$$f(t) = (t - \alpha)q(t).$$

§1. THE EUCLIDEAN ALGORITHM

- **Corollary 1.3.** *Let K be a field such that every non-constant polynomial in $K[t]$ has a root in K. Let f be such a polynomial. Then there exist elements $\alpha_1, \ldots, \alpha_n \in K$ and $c \in K$ such that*

$$f(t) = c(t - \alpha_1) \cdots (t - \alpha_n).$$

- **Corollary 1.4.** *Let f be a polynomial of degree n in $K[t]$. There are at most n roots of f in K.*

§2. GREATEST COMMON DIVISOR

- **An ideal （理想） of $K[t]$ (polynomial idea):** A subset J of $K[t]$ satisfying
  - $0 \in J$;
  - If $f,\ g \in J$, then $f + g \in J$;
  - If $f \in J$ and $g \in K[t]$ arbitrary, then $gf \in J$.

- An ideal of $K[t]$ is a vector space over K.

- **Example 1.** $\langle f_1, \ldots, f_n \rangle = \{g = g_1 f_1 + \cdots + g_n f_n \,|\, g_i \in K[t]\}$ is an ideal of $K[t]$, called the ideal generated by $f_1, \ldots, f_n$ and we say that $f_1, \ldots, f_n$ are a set of generators （生成元） of the ideal $\langle f_1, \ldots, f_n \rangle$.

- $f_i \in < f_1, \ldots, f_n >$

- **Example 2.**
  - The zero ideal: $J = \{0\}$;
  - The unit ideal: $J = K[t] = \langle 1 \rangle$.

- **Example 3.** $\langle t-1,\ t-2 \rangle = \langle 1 \rangle$.

$$\nparallel$$

$\langle t-1 \rangle$ or $\langle t-2 \rangle$

- **Theorem 2.1.** Let J be an ideal of $K[t]$. Then there exists a polynomial g such that $J = \langle g \rangle$.

  Proof.

- **Remark.**
  - If $J = \langle g \rangle$, then $J = \langle cg \rangle$for any constant c;
  - The generator of J is determined up to a constant: If $J = \langle g_1 \rangle = \langle g_2 \rangle$, then $g_1 = cg_2$ for some constant c.
  - A polynomial is called monic, if its leading coefficient is 1.
  - The monic generator of J is uniquely determined.

§2. GREATEST COMMON DIVISOR

- We say that g divide （整除）f and write $g \mid f$, if $\exists q \in K[t]$, s.t. $f = qg$.
- If $g \mid f$, then $cg \mid f$ for any $0 \neq c \in K$.
- $f \mid f$.
- If $g \mid f$ and $h \mid g$, then $h \mid f$.
- If $h \mid f$ and $h \mid g$, then $h \mid (pf + rg)$ for any p and $r \in K[t]$.
- If $g \mid f$ and $f \mid g$, then $f = cg$ for some $0 \neq c \in K$..

§2. GREATEST COMMON DIVISOR

- We say that g is the greatest common divisor（GCD, 最大公因子） of f_1 and f_2, if:
    - $g \mid f_1$ and $g \mid f_2$;
    - $h \mid f_1$ and $h \mid f_2$ implies $h \mid g$.

- **Theorem 2.2.** Let f_1 and f_2 be non-zero polynomials in $K[t]$. Let g be a generator for the ideal $\langle f_1, f_2 \rangle$. Then g is a GCD of f_1 and f_2.

§2. GREATEST COMMON DIVISOR

- For given $f(t)$ and $g(t)$ in $K[t]$, by Th. 1.1, there exist $q(t)$ and $r(t)$ in $K[t]$ with $\deg q < \deg g$, such that: $f(t) = q(t)g(t) + r(t)$.

- GCD(f, g)=GCD(g, r); $\langle f, g \rangle = \langle g, r \rangle$

- Euclidean Algorithm for Finding GCD of $f_1, f_2 \in K[t]$.

-

§2. GREATEST COMMON DIVISOR

- **Theorem.** Let d be a GCD of $f_1, f_2 \in K[t]$. Then, there exist $p,\ q \in K[t]$, such that
$$p(t)f_1(t) + q(t)f_2(t) = d(t)\,.$$

§2. GREATEST COMMON DIVISOR

§2. GREATEST COMMON DIVISOR

- Euclidean Algorithm for Finding GCD
- GCD$(t^4 - t^3 - t^2 + 2t - 1,\ t^3 - 2t + 1)$

§2. GREATEST COMMON DIVISOR

- **Remark 2.** If $f_1, \ldots, f_n$ are non-zero polynomials, and if g is a generator for the ideal $\langle f_1, \ldots, f_n \rangle$, then g is a GCD of $f_1, \ldots, f_n$.
- **Remark 1.**
  - The greatest common divisor is determined up to a non-zero constant multiple.
  - The monic GCD is uniquely determined.
- Polynomials $f_1, \ldots, f_n$ whose GCD is 1 are said to be relatively prime（互素）.

§2. GREATEST COMMON DIVISOR

- Theorem. f and g in $K[t]$ have no common divisor with positive degree iff there exist p and q in $K[t]$, such that:

$$p(t)f(t) + q(t)g(t) = 1.$$

- Corollary. f and g in $C[t]$ have no common root iff there exist p and q in $C[t]$, such that:

$$p(t)f(t) + q(t)g(t) = 1.$$

§2. GREATEST COMMON DIVISOR

- **Theorem.** f and g in $K[t]$ have a common divisor with positive degree iff there exist p and q in $K[t]$, with $\deg(p) < \deg(g)$ and $\deg(q) < \deg(f)$, such that $p(t)f(t) + q(t)g(t) = 0$.

§2. GREATEST COMMON DIVISOR

- **Corollary.** f and g in $C[t]$ have a common root in C iff there exist p and q in $C[t]$, with $\deg(p) < \deg(g)$ and $\deg(q) < \deg(f)$, such that $p(t)f(t) + q(t)g(t) = 0$.
-

§2. GREATEST COMMON DIVISOR

- Resultant （结式） of f and g: res(f, g)
-

§2. GREATEST COMMON DIVISOR

- Theorem. f and g in $K[t]$ have a common divisor with positive degree iff $\operatorname{res}(f, g) = 0$.
-

§2. GREATEST COMMON DIVISOR

- **Corollary.** f and g in C[t] have a common root in C iff res(f, g)=0.

- **Discriminant （判别式）of f**: des(f)=res(f, f').

- f has a multiple root in C iff des(f)=0.

-

§2. GREATEST COMMON DIVISOR

- Homework.
- §1, 1(b), 2, 4;
- §2, 2, 4.
- Compute GCD$(t^6 + t^5 + 3t^4 + 3t^3 + 3t^2 + 2t + 2,\ 2t^4 + t^3 + 5t^2 + 2t + 2)$ by the Euclidean algorithm.