Polynomial Ideals

Euclidean algorithm

Multiplicity of roots

Ideals in F[x].

Euclidean algorithms

- Lemma. f,d nonzero polynomials in F[x]. deg d ≤ deg f. Then there exists a polynomial g in F[x] s.t. either f-dg=0 or deg(f-dg)<deg f.
- Proof of lemma:

$$\begin{aligned} f &= a_m x^m + \sum_{i=0}^{m-1} a_i x^i, a_m \neq 0 \\ d &= b_n x^n + \sum_{i=0}^{n-1} b_i x^i, b_n \neq 0, m \geq n \end{aligned}$$

$$\begin{aligned} f - (a_m/b_n)x^{m-n}d &= c_{m-1}x^{m-1} + \ldots + c_0 \\ \deg(f - (a_m/b_n)x^{m-n}d) &< \deg f \\ \text{or}\, f - (a_m/b_n)x^{m-n}d &= 0 \end{aligned}$$

$$g = (a_m/b_n)x^{m-n}$$

Theorem 4. f, d in F[x]. d ≠0. There exists q,r in F[x] s.t.

(i) f=dq+r

(ii) r=0 or deg r < deg d.

This is the Euclidean algorithm.

- Proof of Theorem 4. If f=0 or deg f < deg d, take q=0, and r=f.
  - As sum deg f > deg d.
  - ∃ g in F[x] s.t.
    (i) deg(f-dg)< deg f or (ii) f-dg=0.
  - Case (i) We find h such that
    - deg(f-dg-dh)<deg f-dg or f-d(g+h)=0.
      …..
    - f-d(g+h+h' +…+$h^{(n)}$) = r with deg r < deg d or =0.
    - Thus f= dq+r, r=0 or deg r < deg d.

- Uniqueness: $f=dq+r$, $f=dq'+r'$.
  - deg r < deg d.
  - Suppose $q-q' \neq 0$ and $d \neq 0$.
  - $d(q'-q)=r'-r$.
  - $\deg d + \deg(q'-q)=\deg(r'-r)$
  - But deg r', deg r < deg d. This is a contradiction.
  - $q'=q$, $r'=r$.

- f=dg, d divides f. f is a multiple of d. g is a quotient of f.
- Corollary. f is divisible by (x-c) iff f(c)=0.
- Proof: f=(x-c)q+r, deg r=0, r is in F. f(c)= 0.q(c)+r. f(c)=0 iff r=0.
- Definition. c in F is a root of f iff f(c)=0.
- Corollary. A polynomial of degree n over a field F has at most n roots in F.
  - Proof: f=(x-a)g if a is a root. Deg g < deg f. By induction g has at most n-1 roots. F has at most n roots.

Multiplicity of roots

- Derivative of $f=c_0+c_1x+\ldots+c_nx^n$.
  - $f'=Df=c_1+2c_2x+\ldots+nc_nx^{n-1}$.
  - $f''=D^2f=DDf$
- Taylors formula: F a field of char 0. f a polynomial.

$$f(x)=\sum_{k=0}^{n}\frac{D^kf(c)}{k!}(x-c), c\in F$$

- Proof:

$$(a+b)^m = \sum_{k=0}^{m} \binom{m}{k} a^{m-k} b^k$$

$$\binom{m}{k} = \frac{m!}{k!(m-k)!} = \frac{m(m-1)\cdots(m-k+1)}{1\cdot 2\cdots k}$$

$$\begin{aligned} x^m &= (c+(x-c))^m \\ &= \sum_{k=0}^{m} \binom{m}{k} c^{m-k}(x-c)^k \\ &= c^m + mc^{m-1}(x-c) + \cdots + (x-c)^m \\ x^m &= \sum_{k=0}^{m} \frac{D^k x^m}{k!}(c)(x-c)^k \end{aligned}$$

$$f(x) = \sum_{m=0}^{n} a_m x^m$$

$$D^k f(c) = \sum_{m=0}^{n} a_m (D^k x^m)(c)$$

$$\sum_{k=0}^{n} \frac{D^k f(c)}{k!}(x-c)^k = \sum_{k=0}^{n} \sum_{m=0}^{n} a_m \frac{D^k x^m(c)}{k!}(x-c)^k$$

$$= \sum_{m=0}^{n} a_m \sum_{k=0}^{n} \frac{D^k x^m(c)}{k!}(x-c)^k = \sum_{m=0}^{n} a_m x^m = f$$

- Multiplicity of roots: c is a zero of f. The multiplicity of c is largest positive integer r such that $(x-c)^r$ divides f.
- Theorem 6: F a field of char 0. deg f ≤n.
  - c is a root of f of multiplicity r iff
  - $D^k f(c) = 0$, $0 \le k \le r-1$, and $D^r f(c) \ne 0$.
- Proof: (->) c mult r. $f=(x-c)^r g$, $g(c) \ne 0$.

$$
\begin{aligned}
f(x) &= (x-c)^r \left(\sum_{m=0}^{n-r} \frac{D^m g}{m!}(c)(x-c)^m \right) \\
&= \sum_{m=0}^{n-r} \frac{D^m g}{m!}(c)(x-c)^{m+r} \\
&= \sum_{k=0}^{n} \frac{D^k f(c)}{k!}(x-c)^k
\end{aligned}
$$

- By uniqueness of polynomial expansions:

$$
\begin{aligned}
\frac{D^k f(c)}{k!} &= 0, 0 \le k \le r-1 \\
&= \frac{D^{k-r} g}{(k-r)!}, r \le k \le n \\
\frac{D^o g(c)}{0!} &= g(c) \neq 0
\end{aligned}
$$

- (<-) $D^k f(c) = 0$, $0 \le k \le r-1$.
  - By Taylors formula, $f = (x-c)^r g$, $g(c) \neq 0$.
  - r is the largest integer such that $(x-c)^r$ divides f.

- Ideals: This is an important concept introduced by Dedekind in 1876 as a generalization of numbers….
- One can add and multiply ideals but ideals are subsets of F[x].
- Ideals play an important role in number theory and algebra. In fact useful in the Fermat conjecture and in algebraic geometry.
- Search “ideal in ring theory”. en.wikipedia.org/wiki/Main_Page

- Definition: An ideal in F[x] is a subspace M of F[x] such that fg is in M whenever f is in F[x] and g is in M.
- General ring theory case is not needed in this book.
- Example: Principal ideals
  - d a polynomial
  - M = dF[x] ={df|f in F[x]} is an ideal.
    - c(df)+dg = d(cf+g).
    - fdg= d(fg)
  - If d in F not 0, then dF[x]=F[x].
  - F[x] is an ideal
  - M is a principal ideal generated by d.
    - (d can be chosen to be monic always)

- Example: $d_1, d_2, \ldots, d_n$ polynomials in F[x]. $\langle d_1F[x], d_2F[x], \ldots, d_nF[x] \rangle$ is an ideal.
- Proof:
  - $g_1 = d_1f_1 + \ldots + d_nf_n, g_2 = d_1h_1 + \ldots + d_nh_n$ in M
    - $cg_1 + g_2 = d_1(cf_1 + h_1) + \ldots + d_n(cf_n + h_n)$ is in M.
  - $g = d_1f_1 + \ldots + d_nf_n$ is in M and f in F[x].
    - $fg = d_1ff_1 + \ldots + d_nff_n$ is in M

- Ideals can be added and multiplied like numbers:
  - $I+J=\{f+g \mid f \in I,\ g \in J\}$
  - $IJ = \{a_1b_1+\ldots+a_nb_n \mid a_i \in I,\ b_i \in J\}$
- Example:
  - $\langle d_1F[x], d_2F[x], \ldots, d_nF[x] \rangle = d_1F[x]+d_2F[x]+\ldots+d_nF[x]$.
  - $d_1F[x]d_2F[x] = d_1d_2F[x]$.

- Theorem: F a field. M any ideal. Then there exists a unique monic polynomial d in F[x] s.t. M=dF[x].
- Proof: M=0 case: done
  - Let M≠0. M contains some non-zero poly.
  - Let d be the minimal degree one.
  - Assume d is monic.
  - If f is in M, f = dq+r. r=0 or deg r < deg d.
  - Since r must be in M and d has minimal degee, r=0.
  - f=dq. M=dF[x].

- Uniqueness: M=dF[x]=gF[x]. d,g monic
  - There exists p, q s.t. d = gp, g=dq.
  - d=dpq. deg d = deg d + deg p + deg q.
  - deg p= deg q=0.
  - d, q monic. p,q=1.
- Corollary: $p_1,\ldots,p_n$ polynomials not all 0. Then There exists unique monic polynomial d in F[x] s.t.
  - (i) d is in $< p_1F[x],\ldots, p_nF[x] >$.
  - (ii) d divides each of the p_is.
  - (iii) d is divisible by every polynomial dividing all p_is. (i.e., d is maximal such poly with (i),(ii).)

- Proof: (existence) Let d be obtained by $M=p_1F[x]+\ldots+p_nF[x] = dF[x]$.
  - (ii) Thus, every f in M is divisible by d.
  - (i) d is in M.
  - (iii) Suppose p_i/f, $i=1,\ldots,n$.
  - Then $p_i=fg_i$ $I=1,\ldots,n$
  - $d= p_1q_1+\ldots+p_nq_n$ since d is in M.
  - $d= fg_1q_1+\ldots+fg_nq_n =f(g_1q_1+\ldots+g_nq_n)$
  - d/f

- (Uniqueness)
  - Let d' satisfy (i),(ii).
  - By (i) for d and (ii) for d', d' divides d.
  - By (i) for d' and (ii) for d, d divides d'.
  - Thus, cd'=d, c in F. d' satisfies (iii) also.
- Remark: Conversely, (i)(ii)(iii) -> d is the monic generator of < $p_1F[x]$,…, $p_nF[x]$ >.

- Definition: $p_1F[x]+\ldots+p_nF[x] = dF[x]$. We define $d=\gcd(p_1,\ldots,p_n)$
- $p_1,\ldots,p_n$ is relatively prime if gcd=1.
- If gcd=1, there exists $f_1,\ldots,f_n$ s.t. $1=f_1p_1+\ldots+f_np_n$.

- Example: $gcd(x+2, x^2+8x+16)$

$$x^2+8x+16=(x+2)(x+6)+4$$

$$4 \in M, 1 \in M, M = F[x]$$

$$gcd(x+1, x^2+8x+16)=1$$

$$1=(-1/4)(x+6)(x+2)+(1/4)(x^2+8x+16)$$

4.5. Prime Factorization of a polynomial

- f in F[x] is reducible over F if there exists g,h s.t. f=gh. Otherwise f is irreducible.
- Example 1: x^2+1 is irreducible in R[x].
  - Proof: $(ax+b)(cx+d)= x^2+1$, a,b,c,d in R
  - $=acx^2 + (bc+ad)x + bd$.
  - ac=1, bd=1, bc+ad=0. c=1/a, d=1/b. b/a+a/b=0. $(b^2+a^2)/ab=0$ -> a=0, b=0.

- $X^2+1=(x+i)(x-i)$ is reducible in C[x].

- A prime polynomial is a non-scalar, irreducible polynomial in F[x].
- Theorem 8. p.f,g in F[x]. Suppose that p is prime and p divides fg. Then p divides f or p divides g.
- Proof: Assume p is monic. (w.l.o.g.)
  - Only divisor of p are 1 and p.
  - Let d = gcd(f,p). Either d=1 or d=p.
  - If d=p, we are done.

- Suppose d=1. f,p rel. prime.
- Since (f, p)=1, there exists f_0,p_0 s.t. $1=f_0f+ p_0p$.
- $g=f_0fg+ p_0pg = (fg)f_0 + p(p_0g)$.
- Since p divides fg and p divides $p(p_0g)$, p divides g.

• Corollary. p prime. p divides $f_1f_2\ldots f_n$. Then p divides at least one f_i.

- Proof: By induction.

- Theorem 9. F a field. Every nonscalar monic polynomial in F[x] can be factored into a product of monic primes in F[x] in one and, except for order, only one way.
- Proof: (Existence)In case deg f =1. f=ax +b=x+b form. Already prime.
  - Suppose true for degree < n.
  - Let deg f=n>1. If f is irreducible, then f is prime and done.

- Otherwise, f=gh. g,h nonscalar, monic.
- deg g, deg h < n. g,h factored into monic primes by the induction hypothesis.
- F= $p_1p_2\ldots p_n$. p_i monic prime.

• (Uniqueness) f= $p_1p_2\ldots p_m=q_1q_2\ldots q_n$.

- p_m must divide q_i for some i by above Cor.
- q_i p_m are monic prime -> $q_i=p_m$
- If m=1 or n=1, then done.
- Assume m,n > 1.
- By rearranging, $p_m=q_n$.
- Thus, $p_1\ldots p_{m-1}=q_1\ldots q_{n-1}$. deg < n.
- By induction $\{p_1,\ldots,p_{m-1}\}=\{q_1,\ldots,q_{n-1}\}$

- $$f = p_1^{n_1} \ldots p_r^{n_r}$$
  primary decomposition of f.
- Theorem 10. $$f = p_1^{n_1} \ldots p_k^{n_k}$$
- $$f_j = f/p_j^{n_j} = \prod_{i \neq j} p_i^{n_i}$$
  Then $f_1, \ldots, f_k$ are relatively prime.
- Proof: Let $g = \gcd(f_1, \ldots, f_k)$.
  - g divides f_i for each i.
  - g is a product of p_is.
  - g does not have as a factor p_i for each i since g divides f_i.
  - g=1.

- Theorem 11: Let f be a polynomial over F with derivative f'. Then f is a product of distinct irreducible polynomial over F iff f and f' are relatively prime.
- Proof: (<-) We show If f is not prod of dist polynomials, then f and f' have a common divisor not equal to a scalar.
  - Suppose $f=p^2h$ for a prime p.
  - $f' = p^2h' + 2pp'h$.
  - p is a divisor of f and f'.
  - f and f' are not relatively prime.

- (->) $f=p_1\ldots p_k$ where $p_1,\ldots,p_k$ are distinct primes.
  - $f' = p_1' f_1+p_2' f_2+\ldots.+p_k' f_k$.
  - Let p be a prime dividing both f and f' .
  - Then $p=p_i$ for some i (since f|p).
  - p_i divides f_j for all $j \neq i$ by def of f_i.
  - p_i divides $f' =p_1' f_1+p_2' f_2+\ldots+p_k' f_k$.
  - p_i divides $p_i' f_i$ by above two facts.
  - p_i can't divide p_i' since deg p_i' < deg p_i.
  - p_i can't divide f_i by definition. A contradiction.
  - Thus f and f' are relatively prime.

- A field F is algebraically closed if every prime polynomial over F has degree 1.

$$f = c(x - c_1)^{m_1} \cdots (x - c_k)^{m_k}$$

- F=R is not algebraically closed.
- C is algebraically closed. (Topological proof due to Gauss.)
- f a real polynomial.
  - If c is a root, then $\bar{c}$ is a root.
  - f a real polynomial, then roots are

$$\{t_1, ..., t_k, c_1, \bar{c}_1, ..., c_r, \bar{c}_r\}, t_i \in R, c_j \in C - R$$

- f is a product of $(x\text{-}t_i)$ and p_js.

$$p_i := (x - c_i)(x - \bar{c}_i) = x^2 - (c_i + \bar{c}_i) + c_i\bar{c}_i$$

- f is a product of 1st order or 2nd order irreducible polynomials.