Polynomial Algebras:

SEM: Advanced topics in linear algebra
UZH, FS 18
Carina Capol

In the whole summary, Γ is a field of characteristic zero.

1. Basic properties:

Def 1.1: A polynomial over Γ is an infinite sequence $f = (\alpha_0, \alpha_1, \dots, \alpha_n, \dots)$ with $\alpha_\nu \in \Gamma$ s.t. only finitely many α_ν are different from zero.

Let $f = (\alpha_0, \alpha_1, \dots, \alpha_n, \dots)$ and $g = (\beta_0, \beta_1, \dots)$ be two polynomials. Then we define the sum and product of two polynomials by:

$$f+g := (\alpha_0+\beta_0, \alpha_1+\beta_1, \dots, \alpha_n+\beta_n, \dots)$$

$$fg := (\gamma_0, \gamma_1, \dots, \gamma_n, \dots) \text{ with } \gamma_k = \sum_{i+j=k} \alpha_i \beta_j$$

Rem: With these two operations the set of all polynomials over Γ is a commutative associative algebra

Def 1.2: The algebra from the remark is called the polynomial algebra over Γ and is denoted by $\Gamma[t]$ with its unit element $1 := (1, 0, \dots)$

Rem: $i: \Gamma \to \Gamma[t]$, $\alpha \mapsto (\alpha, 0, \dots)$ is an injective homomorphism of algebras.

Def 1.3: $t := (0, 1, 0, \dots)$

Rem: From def 1.3 $\Rightarrow t^k = (\overbrace{0, \dots, 0}^{k \text{ times}}, 1, 0, \dots)$ for $k = 0, 1, \dots$

Thus every polynomial f can be written in the form

(*) $f = \sum_{i \geq 0} \alpha_i t^i$ with $\alpha_i \in \Gamma$, where only finitely many α_i are different from zero.

t^k linearly independent $\Rightarrow$ (*) is unique.

$\Rightarrow$ these elements form a basis of the vector space $\Gamma[t]$

Def 1.4: Let $f = \alpha_0 + \alpha_1 t + \dots + \alpha_n t^n \neq 0$ with $\alpha_n \neq 0$. Then

- α_n is called the leading coefficient of f
- If $\alpha_n = 1$, f is called monic
- $\alpha_0 \in \Gamma$ is called the scalar term.
- n is called the degree of f.

Facts: Let $f = \sum_{i=0}^{n} a_i t^i$ and $g = \sum_{i=0}^{m} \beta_i t^i$.

1) If γ is the leading coefficient of fg, then $\gamma = a_n \beta_m$. $(f, g \neq 0)$
2) $f, g \neq 0 \overset{1)}{\Rightarrow} fg \neq 0$
3) The map $\varepsilon: \Gamma[t] \to \Gamma$, $f \mapsto a_0$ is a surjective homomorphism.
4) If $f, g \neq 0 \Rightarrow \deg(f+g) \leq \max(\deg(f), \deg(g))$ and $\deg(fg) = \deg(f) + \deg(g)$.

Def 1.5: A polynomial of the form $a_n t^n$ with $a_n \neq 0$ is called a <u>monomial of degree n</u>.

Rem: Let A be any associative algebra with unit element e and fix $a \in A$.
Then the map $1 \mapsto e$, $t \mapsto a$ can be extended in a unique way to a algebra homomorphism $\Phi: \Gamma[t] \to A$.
Notice, that $1, t$ generate $\Gamma[t] \Rightarrow \Phi$ unique.

Def 1.6: We denote by $\Gamma(a)$ the image of $\Gamma[t]$ under Φ.
Notice, that $\Gamma(a)$ is a subalgebra of A generated by e and a.
The elements of $\Gamma(a)$ are called <u>polynomials in a</u> and are denoted by $f(a)$.

Rem: $\Phi: f \to f(a)$ induces a monomorphism $\overline{\Phi}: \Gamma[t]/\ker(\Phi) \to A$.
Notice, if A is generated by e and $a \Rightarrow \Phi$ is surjective $\Rightarrow \overline{\Phi}$ surjective $\Rightarrow \overline{\Phi}$ is an isomorphism.

EX: Let $A \in \Gamma[t]$ and $g = \sum_{\nu} \beta_\nu t^\nu$ a polynomial.
Then $f(g) = \sum_{\nu} a_\nu \left(\sum_{\nu} \beta_\nu t^\nu\right)^\nu = \sum_{w} \gamma_w t^w$
In particular, $\gamma_0 = \sum_{\nu} a_\nu \beta_0^\nu = f(\beta_0)$
$\Rightarrow \varepsilon(f(g)) = f(\varepsilon(g))$, $f, g \in \Gamma[t]$, with ε from Fact 3).
i.e. the scalar term of $f(g)$ is the same as f of the scalar term of g.

2. Ideals and divisibility:

Lemma 2.1: (Euclid algorithm)

Let $f \neq 0$ and $g \neq 0$ be two polynomials.
Then there exist polynomials q and r, such that
$f = gq + r$ and $\deg(r) < \deg(g)$ or $r = 0$.

EX: Let $f = 6x^2 + 4x + 2$ and $g = 2x + 2$. Then we can find q, r s.t. $f = gq + r$
$\Rightarrow q = x + 1, \; r = 4x^2$

Prop 2.1: Every ideal in $\Gamma[t]$ is principal.

Proof: Let I be the given ideal and assume $I \neq 0$. Let h be a manic polynomial of minimum degree in I.
We need to show that $I = I_h$.
- $I_h \subset I$ is clear.
- Let $f \in I$ arbitrary. Then by the euclid algorithm $\exists\, q, r$ s.t. $f = hq + r$ with $\deg(r) < \deg(h)$ or $r = 0$.
  Since $f, h \in I \Rightarrow r = f - hq \in I$
  If $r \neq 0 \Rightarrow \deg(r) \geq \deg(h)$ ↯
  $\Rightarrow r = 0 \Rightarrow f = hq \Rightarrow f \in I_h$
  Since f arbitrary $\Rightarrow I_h \supset I$ ▨

Def 2.1: Let f and g be non-zero polynomials.
We say that <u>g divides f</u> or <u>f is a multiple of g</u>, if there exists a polynomial h, such that $f = g \cdot h$.
If g divides f we write $g \mid f$.

Rem: f is a multiple of $g \iff f \in I_g$

Facts:
- $h \mid g$ and $g \mid f \Rightarrow h \mid f$
- $f \mid g$ and $g \mid f \Rightarrow f = g$

Def 2.2: Let f and g be two manic polynomials and consider the ideal $I_f + I_g$. Then by prop. 2.1 there exists a unique manic polynomial $h = f \vee g$, such that $I_h = I_f + I_g$
We call $f \vee g$ the <u>greatest common divisor</u> of f and g

Rem: If $h \mid f$ and $h \mid g \Rightarrow I_f \subset I_h, I_g \subset I_h \Rightarrow I_{f \vee g} \subset I_h \Rightarrow h \mid f \vee g$

Def 2.3: A polynomial f, whose only divisors are scalers and scalar multiples of f, is called <u>irreducible</u> or <u>prime</u>.

EX: $\Gamma = \mathbb{R}$. Then $f = x^2 + 1$ is irreducible.

Def 2.4: We denote by $f_1 \vee \dots \vee f_r$ the greatest common divisor of a finite number of monic polynomials f_i, $i = 1, \dots, r$.
It is characterized by the relation

$$I_{f_1 \vee \dots \vee f_r} = I_{f_1} + \dots + I_{f_r}.$$

We call f_i relatively prime, if $f_1 \vee \dots \vee f_r = 1$.

Def 2.5: Analog as in def. 2.2, let f and g be two monic polynomials and consider the ideal $I_f \cap I_g$. Then by prop. 2.1. there exists a unique monic polynomial $h = f \wedge g$, such that $I_h = I_f \cap I_g$
$f \wedge g$ is called the least common multiple of f and g.
We denote by $f_1 \wedge \dots \wedge f_r$ the least common multiple of a finite number of monic polynomials f_i, $i = 1, \dots, r$. and is defined by the equation

$$I_{f_1 \wedge \dots \wedge f_r} = I_{f_1} \cap \dots \cap I_{f_r}.$$

Prop. 2.2: If $f = f_1 \vee \dots \vee f_r$ (greatest common divisor), then there are polynomials $g_1, \dots, g_r$ such that

$$f = \sum_{i=1}^{r} f_i g_i$$

Proof: From def 2.4, an arbitrary $h \in I_f$ can be written as $h = \sum_{i=1}^{r} f_i g_i$. Since $f \in I_f \Rightarrow f = \sum_{i=1}^{r} f_i g_i$ ▨

Corollary 2.1: The polynomials $f_1, \dots, f_r$ are relatively prime iff there exist polynomials $g_1, \dots, g_r$ such that $\sum_{i=1}^{r} f_i g_i = 1$

Proof: "$\Rightarrow$": follows from prop. 2.2.
"$\Leftarrow$": $\sum_{i=1}^{r} f_i g_i = 1 \Rightarrow$ every common divisor of the f_i divides $1 \Rightarrow$ it is a scalar. ▨

Prop. 2.3: Let f_1, f_2 two monic polynomials and $f = f_1 \vee f_2$.
Write $f_i = f h_i$ for $i = 1, 2$.
Then h_1, h_2 are relatively prime and $f_1 \wedge f_2 = f \cdot h_1 \cdot h_2$

Corollary 2.2: If $f_1, \dots, f_r$ monic polynomials are relatively prime, then $f_1 \wedge \dots \wedge f_r = f_1 \cdots f_r$.

Proof: Follows from prop. 2.3. for $r = 2$ and for $r > 2$ by induction.

Rem: Let $\mathcal{P}$ be the set of all monic polynomials in $\Gamma[t]$ together with the zero polynomial. Let us define a partial order in $\mathcal{P}$ by setting:

$f \leq g$ if $g \mid f$ for $f, g \neq 0$

$g \leq 0 \quad \forall g \in \Gamma[t]$

Then with prior chapter, $\mathcal{P}$ becomes a lattice.

Let $\mathcal{J}$ be the set of all ideals in $\Gamma[t]$. Then $\mathcal{J}$ is also a lattice with respect to the partial order given by inclusion.

Let $\Phi : \mathcal{P} \to \mathcal{J}$, $f \mapsto I_f$. Then $f \leq g \Rightarrow I_f \leq I_g$

$\Rightarrow \Phi$ is a lattice homomorphism.

$\overset{\text{Prop. 2.1}}{\Longrightarrow}$ Since Φ is bijective, it is a lattice isomorphism.

Thm 2.1: Every monic polynomial can be written as $f = f_1^{k_1} \cdot \ldots \cdot f_r^{k_r}$, where f_i are distinct irreducible monic polynomials and $\deg(f_i) \geq 1$ for $i = 1, \ldots, r$.

Moreover, the decomposition is unique up to the ordering of the prime factors.

Corollary 2.3: The polynomials, which divide the polynomial $f = f_1^{k_1} \cdot \ldots \cdot f_r^{k_r}$, are precisely the polynomials $g = f_1^{j_1} \cdot \ldots \cdot f_r^{j_r}$ with $j_i \leq k_i$ for $i = 1, \ldots, r$.

Prop. 2.4: Let $f = f_1^{k_1} \cdot \ldots \cdot f_r^{k_r}$ be the decomposition of the monic polynomial f and let $q_i = f_1^{k_1} \cdot \ldots \cdot f_{i-1}^{k_{i-1}} f_{i+1}^{k_{i+1}} \cdot \ldots \cdot f_r^{k_r}$. Then $q_1, \ldots, q_r$ are relatively prime ($q_1 \vee \ldots \vee q_r = 1$) and f is the least common multiple of q_i and $\bigvee_{j \neq i} q_j$ ($q_i \wedge (\bigvee_{j \neq i} q_j) = f$).