Commutative Algebra

Sarfraz Ahmad and Volkmar Welker

Department of Mathematics
COMSATS University, Lahore
and
Fachbereich Mathematik und Informatik
Philipps-Universität Marburg

November/December 2020

Marburg – 23. November 2020

Formalities

- Classes Tuesday 1pm-3pm and Friday 7pm-9pm
- Problem Sets
  - Every two weeks.
  - Will be discussed in one of the classes.
- Final exam, end of December

Rings Revisited

Definition (Commutative ring with 1)

A commutative ring with 1 is a non-empty set R with a

- Addition $+ : R \times R \to R$ and a
- Multiplication $* : R \times R \to R$

such that

- R with $+$ is a commutative group,
- $*$ is associative and commutative,
- there is a neutral element 1 for the multiplication,
- $a(b+c) = ab + ac$ for all $a, b, c \in R$,

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ are rings with the usual addition and multiplication

Example (Polynomial ring)

For a ring R is $R[x]$ the ring of polynomials with coefficients in R in the indeterminate x.

- $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i$ (assume $n \leqslant m$).

$$f = g \Leftrightarrow a_i = b_i, i = 0, \ldots, n \text{ and } b_i = 0$$

  for $n < i \leqslant m$.
- $f = \sum_{i=0}^{n} a_i x^i$

$$\deg(f) = \begin{cases} -\infty & \text{if } f = 0 \\ \max\{i \mid a_i \neq 0\} & \text{otherwise} \end{cases}$$

  is called degree of f.

Rings Revisited

Example (Polynomial ring)

- an $f \in R[x]$ or $f(x) \in R[x]$ has a representation as $f = a_0 + a_1 x + \cdots a_n x^n$ for some $n \geqslant 0$.
- the representation is not unique.
- if we demand that $a_n \neq 0$ then the representation becomes unique for $f \neq 0$.

Definition (Field)

A commutative ring R with 1 is called a field if every non-zero element has a multiplicative inverse.

- a commutative ring with 1 is a field if and only if $R \setminus \{0\}$ is a commutative group.
- examples of fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$,....
- $\mathbb{Z}$ ist not a field, $R[x]$ is not a field.
- we will usually $\mathbb{K}$ to denote a field

Polynomial ring over a field

Lemma

Let $f, g \in \mathbb{K}[x]$ *then*

- $\deg(f+g) \leqslant \max\{\deg(f), \deg(g)\}$.
- $\deg(f \cdot g) = \deg(f) + \deg(g)$.

Convention: We set

$$-\infty + n = n + -\infty = -\infty + -\infty = -\infty < n$$

for all $n \in \mathbb{N}$.

Polynomial ring over a field

Theorem (Division with remainder)

Let $f, g \in \mathbb{K}[x]$ and $g \neq 0$. Then there are polynomials $q, r \in \mathbb{K}[x]$ such that $f = g \cdot q + r$ and $\deg(r) < \deg(g)$.

Beweis.

- $\deg(f) < \deg(g)$: then set $q = 1$ and $r = f$.
- $n = \deg(f) \geqslant m = \deg(g)$:

$$f = \sum_{i=0}^{n} a_i x^i, \quad g := \sum_{i=0}^{m} b_i x^i.$$

We prove the assertion by induction on $n - m$.

Induction Base: $n = m$

Set $q = \frac{a_n}{b_m}$ and $r = f - g\,\frac{a_n}{b_m}$ then

$$f = g\,q + r \text{ and } \deg(r) < \deg(g).$$

Beweis.

Induction Step: $n > m$

Set $q_1 = \frac{a_n}{b_m} x^{n-m}$ and $r_1 = f - \frac{a_n}{b_m} x^{n-m} g$.

Then

$$f = g\, q_1 + r_1 \text{ and } n_1 = \deg(r_1) < \deg(f).$$

If $\deg(r_1) < \deg(g)$ then we are done othwise $0 \leqslant n_1 - m < n - m$.

By induction hypothesis we have q_2 and r_2 scuh that

$$r_1 = g\, q_2 + r_2 \text{ and } \deg(r_2) < \deg(g) = m.$$

$$\begin{aligned} \rightarrow f &= g\, q_1 + r_1 \\ &= g\, q_1 + g\, q_2 + r_2 \\ &= g\,(q_1 + q_2) + r_2 \end{aligned}$$

For $q = q_1 + q_2$ and $r = r_2$ we are done. □

Example

$$f = 2x^4 + x^3 + 2x^2 + 1 \text{ and } g = x^2 + 2x + 1.$$

$$\begin{array}{rrrrl}
2x^4 & + x^3 & + 2x^2 & & + 1 = (x^2+2x+1)\,(2x^2-3x+6)\; -9x-5 \\
-2x^4 & -4x^3 & -2x^2 & & \\ \hline
 & -3x^3 & & & \\
 & 3x^3 & +6x^2 & +3x & \\ \hline
 & & 6x^2 & +3x & +1 \\
 & & -6x^2 & -12x & -6 \\ \hline
 & & & -9x & -5
\end{array}$$

$$q = 2x^2 - 3x + 6 \text{ and } r = -9x - 5.$$

In the polynomial division $f = g\,q + r$ with $\deg(r) < \deg(g)$ we call r the remainder or rest.

Definition

Let $f, g \in \mathbb{K}[x]$ and $g \neq 0$. We say that g divides f if there is q poylnomial $q \in \mathbb{K}[x]$ with $g\,q = f$. We write $g \mid f$.

Definition

Let $f, g \in \mathbb{K}[x]$, $f, g \neq 0$. We say that h is the greatest common divisor of f and g if

- $h|f$, $h|g$ and
- if for some $h' \in \mathbb{K}[x]$ we have $h'|f$ and $h'|g$ then $h'h|h$

We write $\gcd(f, g)$ for the greates common divisor of f and g.

$\rightarrow$ have to show that $\gcd(f, g)$ exists.

Definition (Euclidian Algorithm)

Let $f, g \in \mathbb{K}[x]$ and $g \neq 0$.

- Set $b_0 = f$, $b_1 = g$, $i = 1$
-

(A) Division with remainder $b_{i-1} = b_i\, q_i + r_i$

- $b_{i+1} = r_i$.
- Set $i = i + 1$
- if $b_i = r_{i-1} \neq 0$ then goto (A)
-
- Return b_{i-1}

Equivalent formulation:

$$
\begin{aligned}
f = b_0 &= b_1\, q_1 + r_1 = g\, q_1 + r_1 \\
b_1 &= b_2\, q_2 + r_2 = r_1\, q_2 + r_2 \\
b_2 &= b_3\, q_3 + r_3 = r_2\, q_3 + r_3 \\
&\vdots \\
b_{i-2} &= b_{i-1}\, q_{i-1} + r_{i-1} = r_{i-2}\, q_{i-1} + r_{i-1} \\
b_{i-1} &= b_i\, q_i + 0 = b_i\, q_i + 0
\end{aligned}
$$

$$
b_i = \gcd(f, g).
$$

Polynomial ring over a field

Lemma

For two polynomials $f, g \in \mathbb{K}[x]$, $f, g \neq 0$ *the Euclidian algorithm computes* $\gcd(f, g)$.

Beweis.

Assume the Euclidian algorithm returns b_i.
We claim bd induction on j from $j = i$ to 1 that for $b_0 = f$, $b_1 = g$:

$$b_i = \gcd(b_j, b_{j-1})$$

For $i = 1 : b_i = \gcd(b_1, b_0) = \gcd(g, f)$
Induction base : $j = i$

- $b_{i-1} = b_i q_i \Rightarrow b_i | b_{i,1}, b_i$
- $h | b_{i-1}, h | b_i \Rightarrow h | b_i$

$\Rightarrow b_i = \gcd(b_i, b_{i-1}$ □

Beweis.

Induction step: $j \geqslant 1$

By induction assumption: $b_i = \gcd(b_j, b_{j-1})$.

$$a_{j-1} = b_{j-2} = b_{j-1}q_{j-1} + r_{j-1} = b_{j-1}q_{j-1} + b_j$$

- $b_i = \gcd(b_j, b_{j-1}) \Rightarrow b_i | b_{j-2}$.
- $h | b_{j-2},\ h | b_{j-1} \Rightarrow h | b_j \Rightarrow h | \gcd(b_j, b_{j-1}) = b_i$

$\Rightarrow b_i = \gcd(b_{j-2}, b_{j-1})$. □

Polynomial ring over a field

Example

$$f = (x-1)(x-1)(x^2+1) \text{ and } g = (x-1)(x+1)(x+1)$$

$$x^4 - 2x^3 + 2x^2 - 2x + 1 = \left(x^3 + x^2 - x - 1\right) \cdot \left(x - 3\right) + \left(6x^2 - 4x - 2\right)$$

$$x^3 + x^2 - x - 1 = \left(6x^2 - 4x - 2\right) \cdot \left(\tfrac{1}{6}x + \tfrac{5}{18}\right) + \left(\tfrac{4}{9}x - \tfrac{4}{9}\right)$$

$$6x^2 - 4x - 2 = \left(\tfrac{4}{9}x - \tfrac{4}{9}\right) \cdot \left(\tfrac{27}{2}x + \tfrac{9}{2}\right) + 0$$

$$\gcd(f,g) = \frac{9}{4}(x-1).$$

Corollary

For $f, g \in \mathbb{K}[x]$, $f, g \neq 0$, we have that $\gcd(f,g)$ exists and is unique up to multiplication with $a \in \mathbb{K} \setminus \{0\}$. In addtion there are $u, v \in \mathbb{K}[x]$ such that $\gcd(f,g) = u\,f + v\,g$.

Beweis.

Follows directly from the Euclidian algorithm. □

Polynomial ring over a field

Lemma

Let $f \in \mathbb{K}[x]$ then f has a multiplicative inverse if and only if $f = a$ for some $a \in \mathbb{K} \setminus \{0\}$.

Beweis.

If $a \in \mathbb{K} \setminus \{0\}$ then $a^{-1} \in \mathbb{K}$ thus $a\,a^{-1} = 1$ and a has a multiplicative inverse in $\mathbb{K}[x]$.
Let g be a multiplicative inverse of f:

$\Rightarrow 1 = f\,g$

$$\Rightarrow 0 = \deg(1) = \deg(fg) = \deg(f) + \deg(g).$$

$\deg(f), \deg(g) \in \mathbb{N} \cup \{-\infty\} \Rightarrow \deg(f), \deg(g) = 0 \Rightarrow f = a$ for some $a \in \mathbb{K} \setminus \{0\}$. □

Polynomial ring over a field

Definition

Let $f \in \mathbb{K}[x]$ and $\deg(f) \geqslant 1$. Then we say f is irreducible if $g \mid f$ implies that $g = a\,f$ for some $a \in \mathbb{K} \setminus \{0\}$ or $g = a$ for some $a \in \mathbb{K} \setminus \{0\}$.

Example

- $x - b$ is irreducible for all b
- $\deg(f) = 1 \Rightarrow f$ irreducible.
- $x^2 + 1$ is irreducible in $\mathbb{R}[x]$ but not in $\mathbb{C}[x]$
- f irreducible $\Rightarrow af$ irreducible for any $a \in \mathbb{K} \setminus \{0\}$

Lemma

Every polynomial $f \in \mathbb{K}[x]$ of degree $\deg(f) \geqslant 1$ is a product of irreducible polynomials.

Beweis.

Induction of $\deg(f)$.

Induction base: $\deg(f) = 1$

$\Rightarrow f$ is irreduible $\Rightarrow$ assertion

Induction step: $\deg(f) > 1$

Case: f is irreducible

Then the assertion is trivial.

Case: f is not irreducible

Then there is g such that $g|f$ and $g \neq a\,f \Rightarrow f = g\,h$ for a polynomial h with $\deg(h) \geqslant 1 \to \deg(g), \deg(h) < \deg(f) \xRightarrow{\text{Induction}}$ g and h are products of irrecible polynomials $\Rightarrow$ assertion. $\square$

Lemma

Let g be an irreducible polynomial and $h_1, \ldots, h_s$ polynomials such that $g | h_1 \cdots h_s$ then $g | h_i$ for some $1 \leqslant i \leqslant s$.

Beweis.

Induction of s:

Induction Base: $s = 1, 2$.
$s = 1$: the the assertion is trivial.
$s = 2$: $g | h_1 h_2$ Beweis. If $g \not| h_1 \xrightarrow{g \text{ irreducible}} 1 = \gcd(g, h_1) \Rightarrow$ exist polynomials u and v such that $1 = u\, g + v\, h_1 \Rightarrow$
$h_2 = (u\, g + v\, h_1) h_2 = u\, g\, h_2 + v\, h_1 h_2) \xrightarrow{g | h_1 h_2} g | h_2$. □

Beweis.

Induction Step: $s > 2$.

$g|h_1 \cdots h_s = (h_1 \cdots h_{s-1})h_s \xrightarrow{InductionBase} g|h_1 \cdots h_{s-1}$ or $g|h_s$
$\xrightarrow{Induction} g|h_i$ for some $1 \leqslant i \leqslant s$. □

Theorem

Let $f \in \mathbb{K}[x]$ be of degree $\deg(f) \geqslant 1$. If $f = g_1 \cdots g_r = h_1 \cdots h_s$ for irreducible polynomials $g_1, \ldots, g_r$ and $h_1, \ldots, h_s$ then $r = s$ and after renumbering we have $g_i = a_i h_i$ for some $a_i \in \mathbb{K} \setminus \{0\}$, $i = 1, \ldots, r = s$.

Polynomial ring over a field

Beweis.

$f = g_1 \cdots g_r = h_1 \cdots h_s \Rightarrow g_r | h_1 \cdots h_s \xrightarrow{g_r \text{ irreducible}}$ there is i such that $g_r | h_i \xrightarrow{h_i \text{ irreducible}} h_i = a_i g_i$ for some $a_i \in \mathbb{K} \setminus \{0\}$.

Without restriction of generality : $i = s$.

It follows that $g_1 \cdots g_{r-1} = a_r h_1 \cdots h_{s-1}$

Since $a_i h_1$ is irreducible we get by induction that $r = s$ and $g_i = a_i h_i$ for some $a_i \in \mathbb{K} \setminus \{0\}$. □

Generalization:

Definition

For variables/indeterminates $x_1, \ldots, x_n$ we call $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ for $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$ a monomial.

For $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$ we write $\underline{x}^\alpha$ for $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

Polynomial Rings over a Field

Definition

The $\mathbb{K}[x_1, \ldots, x_n]$ is the $\mathbb{K}$-vectorspace with basis $\{\underline{x}^\alpha \mid \alpha \in \mathbb{N}^n\}$.

We call $f \in \mathbb{K}[x_1, \ldots, x_n]$ or $f(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$ a polynomial.

As a consequence we can write every $f \in \mathbb{K}[x_1, \ldots, x_n]$ uniquely as

$$f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha \cdot \underline{x}^\alpha$$

for $c_\alpha \in \mathbb{K}$ and all but finitely many $c_\alpha = 0$.

Polynomial Rings over a Field

Theorem

The polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ with the vectorspace addition and the multiplication

$$\Big(\sum_{\alpha\in\mathbb{N}} c_\alpha \underline{x}^\alpha\Big) \cdot \Big(\sum_{\alpha\in\mathbb{N}} c'_\alpha \underline{x}^\alpha\Big) = \sum_{\alpha\in\mathbb{N}} \Big(\sum_{\substack{\beta,\beta'\in\mathbb{N}^n \\ \beta+\beta'=\alpha}} c_\beta c'_{\beta'}\Big)\underline{x}^\alpha$$

is a (commutative) ring.

Beweis.

One checks that

$$\mathbb{K}[x_1, \ldots, x_n] = (\cdots(\mathbb{K}[x_1])[x_2])\cdots)[x_n].$$

□