Algebraic Theory I

Thomas Fleming

November 19, 2021

Contents

Lecture 36: Polynomials (2)

Mon 07 May 2018 03:55

Recall. For a commutative ring R, we define the polynomial ring $R\left[x_1, \ldots, x_n\right]$ as formal sums of powers of x_i with coefficients in R.

Moreover, if we have two commutative rings R, R' with a ring homomoprhism $\varphi : R \to \overline{\mathbb{R}}$, then there is a complementary ring homomorphism extending to the polynomial ring:

$$\begin{gathered}\overline{\varphi} : R\left[x\right] \longrightarrow \overline{\mathbb{R}}\left[x\right] \\ \sum_{i=0}^{\infty} \alpha_i x^i \longmapsto \sum_{i=0}^{\infty} \varphi\left(a_i\right) x^i .\end{gathered}$$

Definition 0.1 (Map Space)**.** Now, define $\operatorname{Map}\left(Y \to R\right)$ to be the set of all maps $f : Y \to R$ with R being a commutative ring and Y being an arbitrary set. We equip $\operatorname{Map}\left(Y \to R\right)$ with pointwise operations $\times, +$ such that

$$\begin{gathered}\left(f + g\right)\left(x\right) = f\left(x\right) + g\left(x\right) \\ \left(fg\right)\left(x\right) = f\left(x\right) g\left(x\right) \\ .\end{gathered}$$

These operations induce a ring over $\operatorname{Map}\left(Y \to R\right)$.

Then, we see a polynomial $f \in R\left[x\right]$ defines a corresponding map $\overline{f} \in \operatorname{Map}\left(R \to R\right)$ with $\overline{f}\left(a\right) = \operatorname{ev}_a\left(f\right)$ for all $a \in R$.

Remark. The map $f \mapsto \overline{f}$ need not be injective. See the example $f = x^5 - x$ and $g = 0$ in $\mathbb{F}_5$.

Proposition 0.1. If R is an integral domain, then $R\left[x\right]$ is also an integral domain. Moreover, for nonzero polynomials $f, g \in R\left[x\right]$ we have $\deg\left(fg\right) = \deg\left(f\right) + \deg\left(g\right)$.

This prove is completely trivial hence it is omitted.

Theorem 0.1. If F is a field, then $F[x]$ is a euclidean domain, a principal ideal domain, and a unique factorization domain.

Proof. Applying standard (euclidean) polynomial division with euclidean norm $\deg(f)$ for $f \in F[x]$ yields a euclidean domain (hence a PID and UFD). □

Theorem 0.2. If R is a commutative ring then $R[x]$ is a principal ideal domain if and only if R is a field.

Proof. One direction has already been shown.
Moreover if $R[x]$ is a PID, then R is an integral domain. Hence, if $ab = a$ with $a, b \in R$, then $a = 0$ or $b = 0$, so R is an integral domain as its a subring of $R[x]$.
Now, let $y \in R$be an arbitrary nonzero element. We wish to show y a unit. Let $I = (y, x) \subseteq R[x]$. Then, since $R[x]$ is a Principal ideal domain, we have an $f \in I$ so that $(y, x) = (f)$. Note that we must have $f \neq 0$ as $x \neq 0$ and as $y \in (f)$ we see $y = hf$ for an $h \in R[x]$ which is nonzero. Since R is an integral domain, we see $\deg(f) = \deg(h) = 0$. Hence, f is a nonzero constant $\alpha \in R$. Hence, we have $x \in I = (\alpha)$ so $x = g\alpha$ for some $g \in [x]$. But, R is an integral domain, so $1 = \deg(x) = \deg(\alpha) + \deg(g) = \deg(g)$. So, we have $g = ax + b$ for some nonzero $a \in R \setminus \{0\}$ and $b \in R$. Thus, $x = (ax + b)\alpha = (a\alpha x + b\alpha)$, hence $a\alpha = 1$ and $b\alpha = 0$ by the coefficient property of polynomial rings. Thus,

$$(\alpha) = (f) = I = (y, x) = R[x].$$

Hence, $1 \in (y, x) = R[x](y) + R[x](x)$. So, $1 = g_1 y + g_2 x$ for some $g_1, g_2 \in R[x]$. Hence letting $g_1 = g_{11} + g_{12}x$ and similairly $g_2 = g_{21} + g_{22}x$ for some $g_{11}, g_{12}, g_{21}, g_{22} \in R$, we see $1 = yg_{11}$. So, y is a unit, hence R is a field. □

Corollary 1. If F is a field $F[x, y]$ is not a principal ideal domain.

Proof. $F[x, y] = (F[x])[y]$ and $F[x]$ is not a field (take $f = x$, there is no inverse), so $F[x, y]$ is not a principal ideal domain by applying the previous characterization. □

Theorem 0.3. If F is a field with f being a polynomial having $\deg(f) = n \geq 0$ in $F[x]$. If, $f(a) = 0$ for $a \in R$, then $(x - a) \mid f$. Moreover, f has at most n roots in F.

Proof. Since $f \neq 0$ and f has a zero, we see $\deg(f) \geq 1$. Hence, using polynomial long division yields $f = q(x - a) + r$ for some $q, r \in F[x]$ with $\deg(r) < \deg((x - a))$, hence $\deg(r) \leq 0$, that is r is a constant polynomial.
We see $f(a) = r = 0$, hence $f = q(x - a)$, so $(-a) \mid f$. Letting $a_1, \ldots, a_n$ be distinct real zeros of f, then $(x - a_1) \mid f$ implying $f = f_1(x - a_1)$ with $\deg(f_1) = \deg(f) - 1$. Inducing on the roots a_i, we see that more than n roots

would imply $f = f_1 \cdot f_2 \cdot \ldots \cdot f_n \cdot f_{n+1} \cdot g$ where g is the final polynomial obtained by dividing by $x - a_{n+1}$ and is of degree $\deg(g) = \deg(f) - (n+1) = -1$ implying g is the zero polynomial. But, we have $f = g \prod_{i=1}^{n+1} (x - a_i)$, so $f = 0$ $\lightning$. Hence there are at most n zeroes. $\square$

Lecture 37: Polynomials (3)

Fri 19 Nov 2021 11:30

Theorem 0.4. Let K be a field, with U being a finite multiplicative subgroup. Then it is cyclic.

Proof. Since U is a finite additive group, we see $U = \prod_{i=1}^{n} P_i$ for some sylow p groups P_i. It suffices to show that each subgroup is cyclic as the product of their generators will generate U. Let $x \in P_i$ be an element of maximal order p^m and let $|P_i| = p^n$ for $m \leq n$. Then every $y \in P_i$ has order $\operatorname{ord}(y) \mid p^m$. Hence, they are all roots of $f = x^{p^m} - 1$ which has at most p^m roots, so $p^n = |P_i| \leq p^m$, hence $n \leq m$ so equality holds. So, x has order p^n implying x generates P_i. $\square$

Corollary 2. $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.

Definition 0.2 (Content of a Polynomial)**.** Let R be a UFD with its quotient field K. Let $x \in K$, then there is a unique (up to units) representation $x = \frac{a}{b}$ with $a, b \in R$ being coprime (no prime p has $p \mid a$ and $p \mid b$). Then, for a prime p, define $V_p\left(\frac{a}{b}\right) = V_p(a) - V_p(b)$ where $V_p(x)$ is the power of p in the unique factorization of x. We see one of $V_p(a)$ or $V_p(b) = 0$. Leaving results $V_p(a)$ if $p \mid a$ or $-V_p(b)$ if $p \mid b$. This is called the **p-adic** valuation of $\frac{a}{b}$. Note $V_p(0) := \infty$.
Now, let $f \in K[x]$ with

$$f = \sum_{i=0}^{n} a_i x^i$$

for some $n \in \mathbb{N}$ and $a_i \in K$. Then, we define $V_p(f) = \inf\{V_p(a_i) : i \geq 0\}$. With this, we define the **content** of f to be

$$\operatorname{Cont}(f) = \prod_{p \text{ prime}} p^{V_p(f)}.$$

Remark. The notion of content essentially generalizes the GCD to fraction fields.

Example. Let $R = \mathbb{Z}$ so $K = \mathbb{Q}$, then $V_2\left(\frac{2}{9}\right) = 1$ and $V_3\left(\frac{2}{9}\right) = -2$ and $V_5\left(\frac{2}{9}\right) = 0$.
Then, let $f(x) = \frac{3}{4}x^2 + 6x - 3$, then

$$\operatorname{Cont}(f) = 3 \cdot 2^{-2} = \frac{3}{4}.$$

Since $\operatorname{Cont}(f)$ will always contain all denominators, this allows us to reduce a polynomial over $\mathbb{Q}$ to a rational times a polynomial, $f_1 \in K[x]$ having content $\operatorname{Cont}(f_1) = 1$, hence $f_1 \in R[x]$. $\diamond$

Lemma 0.1. If R is a UFD, with K its quotient field, and $f \in K[x]$, then $\text{Cont}(f) = 1$ implies $f \in R[x]$.

Remark. It is of note that the converse does not hold, take $2x^2 + 4$.

Definition 0.3. For a UFD R and quotient field K, we say $f \in K[x]$ is **primitive** if $\text{Cont}(f) = 1$ (hence $f \in R[x]$).

Lemma 0.2 (Gauss Lemma)**.** Let R be a UFD with K its quotient field. If $f, g \in K[x]$, then $\text{Cont}(fg) = \text{Cont}(f)\,\text{Cont}(g)$.

Proof. Let $c_1 = \text{Cont}(f)$, $c_2 = \text{Cont}(g)$. Then, $f = c_1 f_1$ and $g = c_2 g_1$ for some $f_1, g_1 \in R[x]$ with $\text{Cont}(f_1) = \text{Cont}(g_1) = 1$. So, $fg = \text{Cont}(f)\,\text{Cont}(g)\, f_1 g_1$. Thus, it suffices to show $\text{Cont}(f_1 g_1) = 1$. Since $f_1, g_1 \in R[x]$, we see $f_1 g_1 \in R[x]$. Hence, we need to show no p divides all the coefficients of $f_1 g_1$. Suppose by contradiction that p is a prime dividing all coefficients of $f_1 g_1$. Then, the map

$$\varphi : R[x] \longrightarrow R/(p)[x] = \overline{\mathbb{R}}[x]$$

.

Clearly (p) is a prime ideal, so $\overline{\mathbb{R}}$ is an integral domain with $0 = \varphi(f_1 g_1) = \varphi(f_1)\varphi(g_1)$. Hence either $\varphi(f_1) = 0$ or $\varphi(g_1) = 0$, so WLOG $p \mid a_i$ for all a_i in the representation of f_1, hence $\text{Cont}(f_1) \geq p$ ↯. So the claim holds. □