Algebraic Theory I

Thomas Fleming

November 22, 2021

Contents

Lecture 37: Polynomials (3)

Fri 19 Nov 2021 11:30

Theorem 0.1. 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 1. $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.

Definition 0.1 (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 $V_p(0) \coloneqq \infty$.
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 $\operatorname{Cont}(f) = 1$ implies $f \in R[x]$.

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

Definition 0.2. For a UFD R and quotient field K, we say $f \in K[x]$ is **primitive** if $\operatorname{Cont}(f) = 1$ (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 $\operatorname{Cont}(fg) = \operatorname{Cont}(f)\operatorname{Cont}(g)$.

Proof. Let $c_1 = \operatorname{Cont}(f)$, $c_2 = \operatorname{Cont}(g)$. Then, $f = c_1 f_1$ and $g = c_2 g_1$ for some $f_1, g_1 \in R[x]$ with $\operatorname{Cont}(f_1) = \operatorname{Cont}(g_1) = 1$. So, $fg = \operatorname{Cont}(f)\operatorname{Cont}(g) f_1 g_1$. Thus, it suffices to show $\operatorname{Cont}(f_1 g_1) = 1$. 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 $\operatorname{Cont}(f_1) \geq p$ $\lightning$. So the claim holds. $\square$

Lecture 38: Polynomials (4)

Mon 22 Nov 2021 11:31

Recall. We found the content of a polynomial over a UFD, R, and its quotient field K,essentially being its generalized gcd in order to reduce polynomials in K to polynomials in R.
Moreover, for $f, g \in K[x]$, then $\operatorname{Cont}(f) \cdot \operatorname{Cont}(g) = \operatorname{Cont}(fg)$.

Now, let $f \in R[x]$ with $f = gh$ for $g, h \in K[x]$, K being the quotient field of R. Then, denote $c_g = \operatorname{Cont}(g)$ and $c_h = \operatorname{Cont}(h)$. Then, we find $f = (c_g c_h) g_1 h_1$ for some $h_1, g_1 \in R[x]$.
Then, we see $\operatorname{Cont}(f) = \operatorname{Cont}(h) = c_g c_h$. Since $f \in R[x]$, we see $\operatorname{Cont}(f) \in R$. This implies all factorizations over K admit a factorization over R.

Now, if $f, g \in R[x]$ with $h \in K[x]$ and $f = gh$, then the same argument shows $\mathrm{Cont}(f) = \mathrm{Cont}(g)\mathrm{Cont}(h)$. Hence if f, g are primitive, we find $\mathrm{Cont}(h) \in R$, so $h \in R[x]$.

Theorem 0.2. Let R be a UFD with quotient field K. Let $f \in R[x]$ (we will prove the case f primitive for simplicity, though the non-primitive case is completely analogous). Then, we find f is irreducible in $R[x]$ if and only if f is irreducible in $K[x]$.

Proof. Suppose f irreducible in $K[x]$ but not in $R[x]$. Denote $f = gh$ with $g, h \in R[x]$ being non-units (in $R[x]$).
We know $\mathrm{Cont}(f) = \mathrm{Cont}(g)\mathrm{Cont}(h) = 1$. $f = gh$ is a factorization in K unless g or h is a unit. So, assume WLOG g is a unit in $K[x]$, hence g is constant and $\mathrm{Cont}(g) = g$ hence $g^{-1} = \mathrm{Cont}(h)$. So g is a unit in R $\lightning$.
Now, assume f irreducible in $R[x]$ but not in $K[x]$.
Then $f = gh$ for some $g, h \in K[x]$ being non-units in $K[x]$. Hence, we find g, h are nonconstant polynomials in K. Denote $c_g = \mathrm{Cont}(g), c_h = \mathrm{Cont}(h)$ with $g = c_g g_1$ and $h = g_h h_1$ for $g_1, h_1 \in R[x]$ being primitive, Thus, $f = (c_g c_h) g_1 h_1$ with $c_g, c_h = \mathrm{Cont}(f) \in R[x]$ by hypothesis. Since g, h are nonconstant, g_1, h_1 are nonconstant, hence nonunits and nonzero, so this is a factorization of f over $R[x]$ $\lightning$. So the claim is shown. □

Theorem 0.3. A ring R is a UFD if and only if $R[x]$ is a UFD. Moreover if R be a UFD with quotient field K then $f \in R[x]$ is prime if and only if one of the following hold

1. $f = p \in R$ is a constant with p being prime in R, or
2. f is irreducible over $K[x]$ with $\mathrm{Cont}(f) = 1$.

Proof. We begin by examining the prime elements of $R[x]$. First, we show constant polynomials with prime content are prime in $R[x]$.
Let $f = p \in R[x]$ with $p \in R$ being a prime in R. To show f is prime in $R[x]$, suppose $p \mid gh$ with $g, h \in R[x]$. Then let $c_g = \mathrm{Cont}(g)$ and $c_h = \mathrm{Cont}(h)$ so $g = c_g g_1$ nad $h = c_h h_1$ for primitive $g_1, h_1 \in R[x]$. So, $p \mid (c_g c_h) g_1 h_1$, so $p \mid c_g c_h$. So $p \mid c_g$ or c_h, WLOG suppose the case c_g. Then, $p \mid g$, so p is prime in $R[x]$.
Now, suppose $f \in R[x]$ with f primitive and f irreducible over $K[x]$. Since K is a field, $K[x]$ is a PID, hence UFD, so primes are irreducible, hence f is prime in $K[x]$. Suppose $f \mid gh$ (over R), sometimes denoted $f \mid_R gh$, with $g, h \in R[x]$. Then, $f \mid_{K[x]} gh$, so $f \mid_{K[x]} g$ or h. Assume WLOG the case g and suppose $f = gt$ for some $t \in K[x]$. Since $\mathrm{Cont}(g), \mathrm{Cont}(f) \in R$ we see $\mathrm{Cont}(t) \in R$, hence $t \in [x]$, so $f \mid_{R[x]} g$, hence f is prime.
Now, let $f \in R[x]$ be prime. First, suppose $f = p \in R$ is a constant polynomial which is prime in $R[x]$. If $p \mid_{R[x]} ab$ with $ab \in R$, then we see $p \mid_R ab$. So, $pq = ab \in R$ for a polynomial q implies $\deg(q) \leq 1$. That is, $p \mid_{R[x]} ab$ and since p is prime in $R[x]$ we find WLOG $p \mid_{R[x]} a$. So, $p \mid_R a$ by a similar argument, and we see $p \in R$ is prime.
Otherwise, suppose the prime $f \in R[x]$ has $\deg(f) \geq 1$. We wish to show

$\mathrm{Cont}(f) = 1$ and f irreducible over $R[x]$. But, $f = \mathrm{Cont}(f) f_1$ with $f_1 \in R[x]$ being primitive and $\deg(f) = \deg(f_1) \geq 1$ implies f_1 is a nonunit (in $R[x]$ and $K[x]$). If $\mathrm{Cont}(f) = 1$ this is a contradiction as f is prime (hence irreducible) over $R[x]$. So, $\mathrm{Cont}(f) = 1$.
Finally, we must show f irreducible over $K[x]$ but the preceding lemma handles precisely this case.
Next class we show the final piece of the theorem, that R is a UFD if and only if $R[x]$ is a UFD. $\square$