Intro to Algebra 2 W1-1

fat

February 21, 2024

Important Dates

- Quiz 1: April 3, Wed.
- Midterm: April 12 Fri.
- Quiz 2: May 31, Fri.
- Final: June 7, Fri.

Grading

- Hw 20%, best out of 10 homeworks
- Quiz 10% each ,midterm, final 30% each.

Will Cover

Chap 9, 13, 14 (Skip 13.3)

Section 10.1, 10.2, 10.3, 12.1

1 9.1 Polynomial Rings

Proposition 1. Assume that R is an ID,

1. $\forall p(x), q(x) \neq 0 \in R[x]$, we have

$$deg(pq) = deg(p) + deg(q)$$

2. $(R[x])^\times = R^\times$

3. $R[x]$ is an ID.

Proof.

1. Say

$$p = a_n x^n + \ldots + a_0$$

$$q = b_m x^m + \ldots + b_0$$

With $a_n, b_m \neq 0$. We have

$$pq = a_n b_m x^{m+n} + \ldots$$

Since R is an ID, $a_n b_m \neq 0$. Thus $deg(pq) = m + n = deg(p) + deg(q)$.

2. Let $f(x) \neq 0 \in R[x]$. By 1., we have either $fg \neq 0$ if $g = 0$ or $deg(fg) = deg(f) + deg(g) \leq deg(f)$ if $g \neq 0$. Thus, if $deg(f) \leq 1$, then fg can never be equal to 1. Now if $deg(f(x)) = 0$, then $f(x) = c$ for some $c \neq 0 \in R$. If $fg = 1$ for some $g \in R[x]$, then g is also a constant polynomial and the constant $d \neq 0 \in R$ satisfies $cd = 1 \Rightarrow c \in R^\times$. $\Rightarrow (R[x])^\times \subset R^\times$. Conversely, it's trivial that $R^\times \subset (R[x])^\times \Rightarrow (R[x])^\times = R^\times$.

3. If $f, g \neq 0 \in R[x]$, then by 1., $fg \neq 0$. $\Rightarrow R[x]$ is an ID.

□

Remark 1. We usually adopt the convention that $deg(0) = -\infty$. If we adopt this convention, then 1. holds for all polynomials. Also, $deg(f + g) \leq max(deg(f), deg(g))$, the reason we chose $deg(0) = -\infty$ instead of $+\infty$.

Proposition 2. Assume that $I \trianglelefteq R$, then

$$R[x]/(I) \simeq (R/I)[x]$$

where $(I) = I[x]$.

Proof.

Consider the ring homomorphism: (called the **reduction homomorphism modulo** I)

$$\phi : R[x] \to ({}^{R}/_{I})[x]$$

Defined by

$$\phi(a_n x^n + \ldots + a_0) = \overline{a_n} x^n + \ldots + \overline{a_0}$$

where $\overline{a_j}$ denotes the coset containing a_j. It's clear that ϕ is surjective with $ker\phi = I[x]$.

$$\Rightarrow {}^{R[x]}/_{(I)} \simeq ({}^{R}/_{I})[x]$$

□

Definition 1.1. A term of the form $x_1^{d_1} \ldots x_m^{d_m}$ in $R[x_1, \ldots, x_m]$ is called a **monomial**. Its degree is defined by $d_1 + \ldots + d_m$. The **degree** of a polynomial $f \in R[x_1, \ldots, x_m]$ is defined to be the largest degree of any of the monomialterms in f with nonzero coefficient. A polynomial $f \in R[x_1, \ldots, x_m]$ is **homogeneous** if every monomial term in f has the same degree. Equivalently, if $f(x_1, \ldots, x_m)$ satisfies $f(\lambda x_1, \ldots, \lambda x_m) = \lambda^d f(x_1, \ldots, x_m) \forall \lambda \in R$, then we say f is homogeneous of degree d.

2 9.2 Polynomial over Fields

Theorem 1. Let F be a field. Then the degree function on $F[x]$ is an Euclidean norm. i.e., $\forall a(x), b(x) \neq 0 \in F[x]$
, $\exists! q(x), r(x) \in F[x]$ s.t.

(i) $a(x) = q(x)b(x) + r(x)$

(ii) $r = 0$ or $deg(r) < deg(b)$

Proof.

Let $b(x)$ be a fixed nonzero polynomial in $F[x]$. We'll prove by induction on $deg(a)$ that the theorem holds. If $deg(x) < deg(b)$ ($a(x)$ could be 0 where $deg(0) = -\infty$). We choose $q(x) = 0$ and $r(x) = a(x)$, so the existence in the theorem holds. Assume the existence holds up to $deg(a) = m-1$, where $m \leq deg(b)$. Let $a(x) = a_m x^m + \ldots + a_0$ bbe a polynomial of $deg(m)$. Let $\tilde{a}(x) = a(x) -$

$\frac{a_m}{b_n}x^{m-n}b(x)$. Then $deg(\tilde{a}(x)) \leq m-1$. By the induction hypothesis, $\exists \tilde{q}(x), \tilde{r}(x) \in F[x]$ s.t.

$$\begin{cases} \tilde{a}(x) = \tilde{q}(x)b(x) + \tilde{r}(x) \\ \tilde{r}(x) = 0 \text{ or } deg(\tilde{r}(x)) < deg(b) \end{cases}$$

Let $q = \tilde{q} + \frac{a_m}{b_n}x^{m-n}$, $r(x) = \tilde{r}(x)$, then

$$a(x) = \tilde{a}(x) + \frac{a_m}{b_n}x^{m-n}b(x)$$

$$= \tilde{q}(x)b(x) + \tilde{r}(x) + \frac{a_m}{b_n}x^{m-n}b(x) = q(x)b(x) + r(x)$$

and the existence in the theorem holds for $a(x)$. $\Rightarrow$ the existence in the theorem holds for all $a(x)$. We now prove the uniqueness. Assue that $a(x) = q_1(x)b(x) + r_1(x) = q_2(x) + b(x) + r_2(x)$ with $r_j(x) = 0$ or $deg(r_j(x)) < deg(b)$.

$$\Rightarrow (q_1(x) - q_2(x))b(x) = r_2(x) - r_1(x)$$

If $r_2(x) - r_1(x) \neq 0$, by Prop. 1,

$$deg(\text{L.H.S.}) = deg(q_1(x) - q_2(x)) + deg(b(x)) \leq deg(b)$$

but $deg(\text{R.H.S.}) < deg(b)$, a contradiction. Thus $r_2(x) = r_1(x)$, $q_2(x) = q_1(x)$. □

Corollary 1. $F[x]$ is a PID and a UFD.

Remark 2. From the proof of ED $\Rightarrow$ PID, we see that if $I \neq 0 \trianglelefteq F[x]$, then $I = (f)$ where $deg(f) = \min_{h(x)\in I, h(x)\neq 0} deg(h(x))$.

3 9.3 Polynomial rings that are UFDs

3.1 Summary

Let R be an ID. Then $R[x]$ is a UFD $\Leftrightarrow$ R is a UFD. (Thus if F is a field, then $F[x_1, \ldots, x_n]$ is a UFD for all n). Note that $\Rightarrow$ is easy. From $(R[x])^\times = R^\times$, we see that a nonzero constant polynomial is an irreducible in $R[x] \Leftrightarrow$ the constant is an irreducible in R. From this, we see that $\Rightarrow$ holds.

Proposition 3 (Gauss lemma)**.** Let R be a UFD (think of R as $\mathbb{Z}$) and K be its field of fractions (see localization mentioned in lectures before). Let $f(x) \in R[x]$. If $f(x)$ is reducible in $K[x]$, then $f(x)$ is reducible in $R[x]$. To be more precise, if $f(x) = A(x)B(x)$ for some $A(x), B(x) \in K[x]$, then $\exists r(x), s(x) \in K^\times$ s.t. $r(x)A(x) \equiv a(x), s(x)B(x) \equiv b(x) \in R[x]$ and $f(x) = a(x)b(x)$ (note that $r(x)s(x) = 1$).

Proof.

Let

$$d_1 = LCM(\text{denominators of coefficients of } A(x))$$

$$d_2 = LCM(\text{denominators of coefficients of } B(x))$$

Let

$$a_0(x) = d_1 A(x)$$

$$b_0(x) = d_2 B(x)$$

Then $a_0(x), b_0(x) \in R[x]$. Let $d = d_1 d_2$, then

$$df(x) = (d_1 A(x))(d_2 B(x)) = a_0(x)b_0(x)$$

Let $d = p_1 p_2 \dots p_k$ be the factorization of d into irreducibles in R. Consider the reduction homomorphism modulo (p_1). The reduction of L.H.S. mod (p_1) is 0. Let $\overline{a_0(x)}$ and $\overline{b_0(x)}$ be the reduction of $a_0(x)$ and $b_0(x)$ modulo (p_1). So $\overline{a_0(x)b_0(x)} = 0$ in $(R/(p_1))[x]$. Since p_1 is an irreducible in R and R is a UFD, p_1 is a prime in $R \Rightarrow (p_1)$ is a prime ideal of $R \Rightarrow R/(p_1)$ is an ID $\Rightarrow (R/(p_1))[x]$ is an ID. Thus $\overline{a_0} = 0$ or $\overline{b_0} = 0$ in $R/(p_1)[x]$. W.L.O.G. we assume $\overline{a_0} = 0 \Rightarrow$ Every coefficient of a_0 is a multiple of p_1. i.e. $a_0(x) = p_1 a_1(x)$ for some $a_1(x) \in R[x]$. Let $b_1(x) = b_0(x)$. Then we have

$$df(x) = a_0(x)b_0(x)$$

$$\Rightarrow p_1 \dots p_k f(x) = p_1 a_1(x) b_1(x)$$

$$p_2 \dots p_k = a_1 b_1$$

Repeat the process with p_2 in place of p_1, we see that $\exists a_2, b_2 \in R[x]$ s.t.

$$p_2 \dots p_k f(x) = p_2 a_2(x) b_2(x)$$

$$\Rightarrow p_3 \dots p_k f(x) = a_2(x) b_2(x)$$

Cotinuing this way we get $f(x) = a(x)b(x)$ for some $a(x), b(x) \in R[x]$. □