MATH146 - 2025-01-27

GEORGE MCNINCH

Contents

1. Polynomials over a field and the division algorithm

1.1. Some general notions for commutative rings.

Definition 1.1.1. If R is a commutative ring with 1 and if $u \in R$ we say that u is a *unit* - or that u is *invertible* - provided that there is $v \in R$ with $uv = 1$; then $v = u^{-1}$.

We write $R^\times$ for the units in R.

A commutative ring R is a *field* provided that every non-zero element is invertible. Thus R is a field if $R^\times = R \setminus \{0\}$.

Proposition 1.1.2. *If R is a commutative, then $R^\times$ is an abelian group (with operation the multiplication in R).*

For any commutative ring R and elements $a, b \in R$ we say that a **divides** b – written $a \mid b$ – if $\exists x \in R$ with $ax = b$.

Proposition 1.1.3. *For $a, b \in R$ we have $a \mid b$ if and only if $b \in \langle a \rangle$.*

Recall that we introduced the principal ideal $\langle a \rangle = aR$ for any commutative ring R and any $a \in R$. In fact, given $a_1, \cdots, a_n \in R$ we can consider the ideal

$$\langle a_1, \cdots, a_n \rangle = \sum_{i=1}^n a_i R$$

defined as

$$\langle a_1, \cdots, a_n \rangle = \left\{ \sum_{i=1}^n r_i a_i | r_i \in R \right\}.$$

It is straightforward to check that $\langle a_1, \cdots, a_n \rangle$ is indeed an ideal of R.

Date: 2025-01-26 14:26:05 EST (george@valhalla).

1.2. **The degree of a polynomial.** Let F be a field and consider the ring of polynomials $F[T]$.

Definition 1.2.1. The *degree* of a polynomial $f = f(T) \in F[T]$ is define to be $\deg(f) = -\infty$ if $f = 0$, and otherwise $\deg(f) = n$ where

$$f = \sum_{i=0}^{n} a_i T^i \quad \text{with each } a_i \in F \text{ and } a_n \neq 0.$$

We have some easy and familiar properties of the degree function:

Proposition 1.2.2. *Let $f, g \in F[T]$.*

(a) $\deg(fg) = \deg(f) + \deg(g)$.
(b) $\deg(f+g) \le \max\{\deg(f), \deg(g)\}$ *and equality holds if* $\deg(f) \neq \deg(g)$.
(c) $f \in F[T]^\times$ *if and only if* $\deg(f) = 0$. *In particular,* $F[T]^\times = F^\times$.

1.3. **The division algorithm.**

Theorem 1.3.1. *Let F be a field, and let $f, g \in F[T]$ with $0 \neq g$. Then there are polynomials $q, r \in F[T]$ for which*

$$f = qg + r$$

and $\deg r < \deg g$.

Proof. First note that we may suppose f to be non-zero. Indeed, if $f = 0$, we just take $q = r = 0$. Clearly $f = qg + r$, and $\deg(r) = -\infty < \deg(g)$ since g is non-zero.

We now proceed by induction on $\deg(f) \ge 0$.

For the base case in which $\deg(f) = 0$, we note that $f = c$ is a constant polynomial; here $c \in F^\times$.

If $\deg(g) = 0$ as well, then $g = d \in F^\times$ and then $c = (c/d)d + 0$ so we may take $q = c/d$ and $r = 0$. Now $\deg(r) = -\infty < \deg(g)$ as required.

If $\deg(g) > 0$, we simply take $q = 0$ and $r = f$: we then have $f = 0 \cdot g + f$ and $\deg(f) = 0 < \deg(g)$ as required.

We have now confirmed the Theorem holds when $\deg(f) = 0$.

Proceeding with the induction, we now suppose $n > 0$ and that the Theorem holds whenever f has degree $< n$. We must prove the Theorem holds when f has degree n.

Since f has degree n, we may write $f = a_n T^n + f_0$ where $a_n \in F^\times$ and $f_0 \in F[T]$ has $\deg(f_0) < n$.

Let us write $g = \deg(g)$; we may write $g = b_m T^m + g_0$ where $b_m \in F^\times$ and $g_0 \in F[T]$ has $\deg(g_0) < m$.

If $n < m$ we take $q = 0$ and $r = f$ to find that $f = qg + r$ and $\deg(r) < \deg(g)$.

Finally, if $m \le n$ we set

$$f_1 = f - (a_n/b_m)T^{n-m}g = a_n T^n + f_0 - \left(\frac{a_n}{b_m} b_m T^n + \frac{a_n}{b_m} T^{n-m} g_0\right) = f_0 - \frac{a_n}{b_m} T^{n-m} g_0.$$

We have $\deg(f_0) < n$ by assumption, and $\deg\left(\frac{a_n}{b_m} T^{n-m} g_0\right) < n$ by the Proposition together with the fact that $\deg(g_0) < m$.

Thus $\deg(f_1) < n$. Now we apply the induction hypothesis to write

$$f_1 = q_1 g + r_1 \quad \text{with } \deg(r_1) < \deg(g).$$

Finally, we have

$$f = f_1 + (a_n/b_m)T^{n-m}g = q_1 g + r_1 + (a_n/b_m)T^{n-m}g = \left(q_1 + (a_n/b_m)T^{n-m}\right) g + r_1$$

so we have indeed written $f = qg + r$ in the required form. $\square$

Corollary 1.3.2. *Let F be a field and let $f \in F[T]$. For $a \in F$, there is a polynomial $q \in F[T]$ for which*

$$f = q(T - a) + f(a).$$

Corollary 1.3.3. *For $f \in F[T]$ an element $a \in F$ is a* ***root*** *of thea polynomial f if and only if $T - a \mid f$ in $F[T]$.*

1.4. **Ideals of the polynomial ring $F[T]$.**

Corollary 1.4.1. *Let F be a field and let I be an ideal of the ring $F[T]$. Then I is a principal ideal; i.e. there is $g \in I$ for which*

$$I = \langle g \rangle = g \cdot F[T].$$

Proof. If $I = \{0\}$ [1] the results is immediate. Thus we may suppose $I \neq 0$.

COnsider the set $\{\deg(g) | 0 \neq g \in I\}$. This is a non-empty set of natural numbers, hence it contains a minimal element by the **well-ordering principle**.

Choose $g \in I$ such that $\deg(g)$ is this minimal degree; we claim that $I = \langle g \rangle$.

Clearly $\langle g \rangle \subseteq I$. To complete the proof, it remains to establish the inclusion $I \subseteq \langle g \rangle$. Let $f \in I$ and use the **Division Algorithm** to write $f = qg + r$ for $q, r \in F[T]$ with $\deg r < \deg g$.

Observe that $f - qg \in I$ so that $r \in I$. Since $\deg r < \deg g$ conclude that $r = 0$. This shows that $f = qg \in \langle g \rangle$ as required, completing the proof. $\square$

Let F be a field, $F[T]$ be the ring of polynomials with coefficients in F, let $f, g \in F[T]$ be polynomials which are not both 0.

Definition 1.4.2. The **greatest common divisor** $\gcd(f, g)$ of the pair f, g is a monic polynomial d such that

(a) $d \mid f$ and $d \mid g$,
(b) if $e \in F[T]$ satisfies $e \mid f$ and $e \mid g$, then $e \mid d$.

Remark 1.4.3. If d, d' are two gcds of f, g then $d \mid d'$ and $d' \mid d$. In particular, $\deg(d) = \deg(d')$ and $d' = \alpha d$ for some $\alpha \in F^\times$. It is then clear that there is no more than one monic polynomial satisfying i. and ii.

Proposition 1.4.4. *Let $f, g \in F[T]$ not both 0* [2].

(a) $\langle f, g \rangle$ is an ideal. According to the previous corollary, there is a monic polynomial $d \in F[T]$ with

$$\langle d \rangle = \langle f, g \rangle.$$

Then $d = \gcd(f, g)$

(b) In particular, $d = \gcd(f, g)$ may be written in the form $d = uf + vg$ for $u, v \in F[T]$.

[1] We will write simply 0 for the ideal $\{0\}$.
[2] Note that f, g are not both 0 if and only if the ideal $\langle f, g \rangle$ is not 0.

Proof. For a., write $I = \langle f, g\rangle = \langle d\rangle$. Since $f, g \in I$, the definition of $\langle d\rangle$ shows that $d \mid f$ and $d \mid g$.

Now suppose that $e \in F[T]$ and that $e \mid f$ and $e \mid g$. Then $f, g \in \langle e\rangle$ which shows that $\langle f, g\rangle \subseteq \langle e\rangle$.

But this implies that $\langle d\rangle \subset \langle e\rangle$ so that $e \mid d$ as required. Thus we see that d is indeed equal to $\gcd(f, g)$.

Since $d \in \langle d\rangle = \langle f, g\rangle$, assertion b. follows from the definition of $\langle f, g\rangle$. □

1.5. **Integral domains and principal ideal domains (PIDs).** Let R be a commutative ring. The non-zero element $a \in R$ is said to be a 0-divisor provided that there is $0 \neq b \in R$ with $ab = 0$.

Example 1.5.1. Let n be a composite positive integer, so that $n = ij$ for integers $i, j > 0$. Consider the elements $[i] = i + n\mathbf{Z}, [j] = j + n\mathbf{Z}$ in the quotient ring $\mathbf{Z}/n\mathbf{Z}$.

Then $[i]$ and $[j]$ are both non-zero since $0 < i, j < n$ so that $n \not| \, i$ and $n \not| \, j$. But $[i] \cdot [j] = [n] = 0$ so that $[i]$ and $[j]$ are 0-divisors of the ring $\mathbf{Z}/n\mathbf{Z}$.

Definition 1.5.2. A commutative ring R is said to be an **integral domain** provided that it has no zero-divisors.

Example 1.5.3.
(a) Any field is an integral domain.
(b) The ring $\mathbf{Z}$ of integers is an integral domain.
(c) If R is an integral domain, the polynomial ring $R[T]$ is an integral domain.
(d) Any subring of an integral domain is an integral domain.
For example, the ring $\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$ of gaussian integers is an integral domain.
(e) $\mathbf{Z}/n\mathbf{Z}$ is not an integral domain whenever n is composite.

Lemma 1.5.4. *Let R be an integral domain and let $a, b, c, \in R$ with $c \neq 0$. If $ac = bc$ then $a = b$.*

Proof. The equation $ac = bc$ implies that $ac - bc = 0$ so that $(a - b)c = 0$ by the distributive property. Since R has no zero divisors and since $c \neq 0$ by assumption, conclude that $a - b = 0$ i.e. that $a = b$. □

Definition 1.5.5. An integral domain R is said to be a **principal ideal domain** (abbreviated PID) provided that every ideal I of R has the form

$$I = \langle a\rangle \quad \text{for some } a \in R;$$

i.e. provided that every ideal of R is principal.

Example 1.5.6.
(a) The ring $\mathbf{Z}$ of integers is a PID.
(b) For any field F, the ring $F[T]$ of polynomials is a PID - this follows from the Corollary to the divison algorithm, above.
(c) The rings $\mathbf{Z}[i]$ and $\mathbf{Z}[\sqrt{2}]$ are PIDs – to see this one can argue that these rings are Euclidean domains and then one proves that any Euclidean domain is a PID.

1.6. **Prime elements in a PID.** Let R be a PID.

For $a_1, \cdots, a_n \in R$ write $\langle a_1, \cdots, a_n\rangle = Ra_1 + \cdots + Ra_n$ for the ideal generated by the a_i, as before.

Our results about gcd in the polynomial ring actually hold in the generality of the PID R. We quickly give the statements:

Definition 1.6.1. Let $a, b \in R$ such that $\langle a, b\rangle \neq 0$. A gcd of a and b is an element $d \in R$ such that

(i) $d \mid a$ and $d \mid b$ ("d is a common divisor of a and b")
(ii) if $e \mid a$ and $e \mid b$ then $e \mid d$. ("any common divisor of a and b divides d)")

Lemma 1.6.2. *If d and d' are* gcd*s of a and b then $d' = ud$ for a unit $u \in R^\times$.*

Proof. Using the definition of gcd we see that $d \mid d'$ and $d' \mid d$. Thus $d' = dv$ and $d = d'u$ for $u, v \in R$.

This shows that $d' = dv = d'uv$. Using cancellation, find that $1 = uv$ so that $u, v \in R^\times$. □

Remark 1.6.3. This definition of course covers the cases when $R = \mathbf{Z}$ and when $R = F[T]$. The main thing to point out is that when $R = \mathbf{Z}$, there is a unique **positive** gcd for any pair $a, b \in \mathbf{Z}$ and when $R = F[T]$ there is a unique **monic** gcd for any pair $f, g \in F[T]$.

For a general PID there need not be a natural choice of gcd, so for $x, y \in R$ we can only speak of $\gcd(x, y)$ up to multiplication by a unit of R.

Proposition 1.6.4. *Let R be a PID and let $x, y \in R$ with $\langle x, y\rangle \neq 0$.*

(a) Since R is a PID, we may write find $d \in R$ with

$$\langle d\rangle = \langle x, y\rangle.$$

Then $d = \gcd(x, y)$.

(b) In particular, $d = \gcd(x, y)$ may be written in the form $d = ux + vv$ for $u, v \in R$.

To prove Proposition 1.6.4 proceed as in the proof of Proposition 1.4.4.

Let R be a PID.

Definition 1.6.5. A non-zero element $p \in R$ is said to be **irreducible** provided that $p \notin R^\times$ and whenever $p = xy$ for $x, y \in R$ then either $x \in R^\times$ or $y \in R^\times$.

Remark 1.6.6. Assume that $p, a \in R$ with p irreducible. Then either $\gcd(p, a) = 1$ or $\gcd(p, a) = p$.

Proposition 1.6.7. *$p \in R$ is irreducible if and only if ($\clubsuit$): whenever $a, b \in R$ and $p \mid ab$ then either $p \mid a$ or $p \mid b$.*

Proof. ($\Rightarrow$): Assume that p is irreducible, suppose that $a, b \in R$ and that $p \mid ab$. We must show that $p \mid a$ or $p \mid b$.

For this, we may as well suppose that $p \not| a$; we must then prove that $p \mid b$. Since $p \not| a$, we see that $\gcd(a, p) = 1$ by the Remark above. Then $ua + vp = 1$ for elements $u, v \in R$.

Now we see that

$$b = 1 \cdot b = (ua + vp) \cdot b = uab + vpb.$$

Since $p \mid ab$ we see that $p \mid uab + vpb$ which proves that $p \mid b$, as required.

($\Leftarrow$): Assume that condition ($\clubsuit$) holds for p. We must show that p is irreducible. For this, assume $p = xy$ for $x, y \in R$; we must show that either $x \in R^\times$ or $y \in R^\times$.

Since $p = xy$, in particular $p \mid xy$ and we may apply ($\clubsuit$) to conclude without loss of generality that $p \mid x$.

Write $x = pa$. We now see that $p = xy = pay$; by cancellation, find that $1 = ay$ so that $y \in R^\times$. We conclude that p is irreducible, as required. □

2. Irreducible polynomials over a field

2.1. Some criteria for irreducibility.

Proposition 2.1.1. *Let F be a field and let $f \in F[T]$ be a polynomial with $\deg(f) \leq 3$. If f has no root in F then f is irreducible.*