Foreword

Usage

- Notes are presented in two columns: main notes on the left, and sidenotes on the right. Main notes will have a larger margin.

- The following is the color code for the notes:

Blue	Definitions
Red	Important points
Yellow	Points to watch out for / comment for incompletion
Green	External definitions, theorems, etc.
Light Blue	Regular highlighting
Brown	Secondary highlighting

- The following is the color code for boxes, that begin and end with a line of the same color:

Blue	Definitions
Red	Warning
Yellow	Notes, remarks, etc.
Brown	Proofs
Magenta	Theorems, Propositions, Lemmas, etc.

- Hyperlinks are underlined in magenta. If your PDF reader supports it, you can follow the links to either be redirected to an external website, or a theorem, definition, etc., in the same document. Note that this is only reliable if you have the full set of notes as a single document, which you can find on:
  `https://japorized.github.io/TeX_notes`

28 Lecture 28 Jul 09th 2018

28.1 Polynomial Ring (Continued)

28.1.1 Factorization of Polynomials (Continued)

Since the actual focus of our study right now is really fields instead of just integral domains, we shall use fields in place of integral domains or commutative rings from here on unless explicitly stated otherwise. So we redefine Definition 49 as follows:

Definition (Division of Polynomials)
Let F be a field and consider $F[x]$. For $f(x), g(x) \in F[x]$, we say that $f(x) \mid g(x)$ if $\exists q(x) \in F[x]$ such that

$$g(x) = q(x)f(x).$$

and restate the last stated proposition as follows:

Proposition 83 ($f(x) \mid g(x) \wedge g(x) \mid f(x) \implies f(x) = g(x)$)

Let F be a field and $f(x), g(x) \in F[x]$ be monic polynomials[1]*. If $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $f(x) = g(x)$.*

Proof
Since $f(x) \mid g(x)$ and $g(x) \mid f(x)$, $\exists r(x), s(x) \in F[x]$ such that

$$g(x) = r(x)f(x) \text{ and } f(x) = s(x)g(x).$$

[1] Note that polynomials being monic is analogous to integers being positive. For example, you (read: I) should try to reiterate the proof below by replacing the monic property with positive integers.

Then

$$f(x) = s(x)r(x)f(x).$$

By Proposition 82, we have that

$$\deg f = \deg s + \deg r + \deg f$$

and so

$$\deg s + \deg r = 0 \implies \deg s = \deg r = 0 \quad \because \deg s, \deg r \geq 0.$$

And so $\exists t \in F$ *such that* $f(x) = tg(x)$. *Since* $f(x)$ *and* $g(x)$ *are monic, we must have* $t = 1$ *and so* $f(x) = g(x)$. □

Proposition 84 (Division Algorithm for Polynomials)

Let F *be a field, and* $f(x), g(x) \in F[x]$ *with* $f(x) \neq 0$. *Then* $\exists ! q(x), r(x) \in F[x]$ *such that*

$$g(x) = q(x)f(x) + r(x)$$

with $\deg r < \deg f$.[2]

Proof

We shall first prove the existence of such a $q(x)$ *and* $r(x)$. *For simplicity, write*

$$\deg f = m \text{ and } \deg g = n.$$

If $n < m$, *then*

$$g(x) = 0f(x) + g(x)$$

and we are done. Suppose that $n \geq m$ *and proceed by induction of* n. *Write*

$$f(x) = a_0 + a_1 x + \ldots + a_m x^m$$
$$g(x) = b_0 + b_1 x + \ldots + b_n x^n.$$

Consider[3]

[2] Note that this includes the case for $r = 0$, and this is yet another reason why we defined $\deg 0 = -\infty$.

[3] We are implicitly using the fact that $x \in Z[x]$.

$$\begin{aligned} g_1(x) &= g(x) - b_n a_m^{-1} x^{n-m} f(x) \\ &= (b_n x^n + \ldots + b_0) - b_n a_m^{-1} x^{n-m} (a_m x^m + \ldots a_0) \\ &= 0x^n + (b_{n-1} - b_n a_m^{-1} a_{m-1}) x^{n-1} + \ldots, \end{aligned}$$

thus either $g_1(x) = 0$ or $g_1(x) \neq 0$, but in any case, $\deg g_1 < n$.

***Case 1**: $g_1(x) = 0$. In this case, we have*

$$g(x) = b_n a_m^{-1} x^{n-m} f(x)$$

and so we can pick

$$\begin{aligned} q(x) &= b_n a_m^{-1} x^{n-m} \\ r(x) &= 0, \end{aligned}$$

and the result follows.

***Case 2**: $g_1(x) \neq 0$. By induction, we can find some $q_1(x), r_1(x) \in F[x]$ such that*

$$g_1(x) = q_1(x) f(x) + r_1(x)$$

with $\deg r_1 < \deg f$. It follows that

$$\begin{aligned} g(x) &= g_1(x) + b_n a_m^{-1} x^{n-m} f(x) \\ &= q_1(x) f(x) + r_1(x) + b_n a_m^{-1} x^{n-m} f(x). \end{aligned}$$

So pick

$$\begin{aligned} q(x) &= q_1(x) + b_n a_m^{-1} x^{n-m} \\ r(x) &= r_1(x) < \deg f, \end{aligned}$$

and so the result follows.

To prove uniqueness, suppose we have

$$q_1(x) f(x) + r_1(x) = q_2(x) f(x) + r_2(x)$$

with $\deg r_1, \deg r_2 < \deg f$. Then

$$r_2(x) - r_1(x) = [q_1(x) - q_2(x)] f(x).$$

If $q_1(x) - q_2(x) \neq 0$, then

$$\deg(r_2 - r_1) = \deg(q_1 - q_2) + \deg f \geq \deg f$$

which is a contradiction since $\deg(r_2 - r_1) < \deg f$. *Thus we must have* $q_1(x) = q_2(x)$ *and so* $r_1(x) = r_2(x)$. □

Proposition 85 (Properties of the Greatest Common Divisor)

Let F *be a field and* $f(x), g(x) \in F[x]$ *with* $f(x) \neq 0 \neq g(x)$. *Then* $\exists! d(x) \in F[x]$ *such that*

1. $d(x)$ *is monic;*
2. $d(x) \mid f(x)$ *and* $d(x) \mid g(x)$;
3. $e(x) \mid f(x) \wedge e(x) \mid g(x) \implies e(x) \mid d(x)$;
4. $\exists u(x), v(x) \in F[x] \quad d(x) = u(x)f(x) + v(x)g(x)$

In this case, we say that $d(x)$ *is the* ***greatest common divisor*** *of* $f(x)$ *and* $g(x)$, *and denote this by* $d(x) = \gcd[f(x), g(x)]$.

Proof

Consider the set

$$X = \{u(x)f(x) + v(x)g(x) : u(x),\, v(x) \in F[x]\}.$$

Since $f(x) = 1 \cdot f(x) + 0 \cdot g(x) \in X$, *the set* X *contains non-zero polynomial and thus contains monic polynomials (since* F *is a field*[4]*). Among all of the monic polynomials, choose*

$$d(x) = u(x)f(x) + v(x)g(x)$$

to have minimal degree. Then we get (1) *and* (4) *in the bag automatically so.* (3) *also follows almost immediately, since*

$$\begin{aligned} & e(x) \mid f(x) \wedge e(x) \mid g(x) \\ & \implies \exists a(x), b(x) \in F[x] \quad f(x) = a(x)e(x) \wedge g(x) = b(x)e(x) \\ & \implies d(x) = u(x)f(x) + v(x) = [u(x)a(x) + v(x)b(x)]e(x) \\ & \implies e(x) \mid d(x). \end{aligned}$$

It remains to prove (2). *By* Proposition 84, *we have that* $\exists q(x), r(x) \in$

[4] This is cause if we have

$$f(x) = a_m x^m + \ldots + a_0$$

Then

$$a_m^{-1} f(x) = x^m + \ldots + a_m^{-1} a_0$$

is a moic polynomial in $F[x]$.

$F[x]$ with $\deg r < \deg f$ such that

$$f(x) = q(x)d(x) + r(x).$$

Then

$$\begin{aligned} r(x) &= f(x) - q(x)d(x) = f(x) - q(x)[u(x)f(x) + v(x)g(x)] \\ &= [1 - q(x)u(x)]f(x) - q(x)v(x)g(x). \end{aligned}$$

Note that if $r(x) \neq 0$, then write $k \neq 0 \in F$ as the leading coefficient of $r(x)$. Since F is a field, we have that $\exists k^{-1} \in F$, and so $k^{-1}r(x)$ is a monic polynomial of X with $\deg(k^{-1}r) < \deg d$, which contradicts the fact that the degree of $d(x)$ is minimal. Thus $r(x) = 0$ and $d(x) \mid f(x)$. Using a similar argument, we can show that $d(x) \mid g(x)$. Therefore, (2) follows. □

Exercise 28.1.1
Reiterate this proof for integers, by removing the '(x)' and replacing instances of monic polynomials with positive integers.