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`

29 Lecture 29 Jul 11th 2018

29.1 Polynomial Ring (Continued)

29.1.1 Factorization of Polynomials (Continued 2)

Note

If $d(x)$ and $d_1(x)$ satisfies Proposition 85, then in particular (3) is satisfied, i.e.

$$d(x) \mid d_1(x) \text{ and } d_1(x) \mid d(x),$$

then since $d_1(x) = d(x)$ by Proposition 83. Thus $d(x)$ is unique and is therefore called the greatest common divisor of $f(x)$ and $g(x)$, denoted by $\gcd\left(f(x), g(x)\right) = d(x)$.

Note that in integers, $p \in \mathbb{Z}$ is prime if $p \geq 2$ and whenever $p = ab$, then $a = \pm 1$ or $b = \pm 1$, where $a, b \in \mathbb{Z}$. We can have an "analogous" notion with polynomials.

Definition 51 (Irreducible Polynomials)

Let F be a field. A non-zero polynomial $l(x) \in F[x]$ is ***irreducible*** *if* $\deg l \geq 1$ *and if*

$$l(x) = l_1(x) l_2(x)$$

for $l_1(x), l_2(x) \in F[x]$, then $\deg l_1 = 0$ *or* $\deg l_2 = 0$ [1].

Polynomials that are not irreducible are called ***reducible polynomials***.

[1] Note that polynomials of degree 0 are the units of $F[x]$.

Proposition 86 (Euclid's Lemma for Polynomials)

Let F be a field and $f(x), g(x) \in F[x]$. If $l(x) \in F[x]$ is irreducible and $l(x) \mid a(x)b(x)$, then $l(x) \mid a(x)$ or $l(x) \mid b(x)$.

This is a good proof for an exercise.

Exercise 29.1.1
Prove Proposition 86.

Proof

Suppose $l(x) \mid f(x)g(x)$ and $l(x) \not| f(x)$. Since $l(x) \not| f(x)$, we have $\gcd[l(x), f(x)] = 1$. Then by Proposition 85, $\exists s(x), t(x) \in F[x]$ such that

$$l(x)s(x) + f(x)t(x) = 1.$$

Multiplying the equation by $g(x)$, and since $F[x]$ is a field, we have

$$l(x)s(x)g(x) + f(x)g(x)t(x) = g(x).$$

Since $l(x) \mid f(x)g(x)$ by assumption, we have that $l(x)$ divides the right hand side, and so it must also divide the left hand side, i.e. $l(x) \mid g(x)$. $\square$

Theorem 87 (Unique Factorization Theorem for Polynomials)

Let F be a field and $f(x) \in F[x]$ with $\deg f \geq 1$. Then we can write

$$f(x) = cl_1(x)l_2(x) \ldots l_m(x)$$

where $c \in F^*$ is a unit, and for $1 \leq i \leq m$, $l_i(x)$ is a irreducible monic polynomial. This factorization is unique up to the order of l_i.

This is, yet again, a good proof for an exercise.

Exercise 29.1.2
Proof Theorem 87.

Proof

We shall only prove for when $f(x)$ is a monic polynomial, for if $f(x)$ is not monic, then it has some leading coefficient $a \neq 1 \in F$. Then since F is a field, we have that $a^{-1}f(x)$ is a monic polynomial for which we can continue our consideration.

Suppose $f(x)$ is a monic polynomial that has the least degree such that it cannot be expressed as a product of irreducible monic polynomials. Clearly, $f(x)$ cannot be irreducible itself, or it would trivially be *expressible as a product of irreducible monic polynomials. Therefore, $\exists s(x), t(x) \in F[x]$ such that*

$$f(x) = s(x)t(x)$$

where $1 \leq \deg s, \deg t \leq \deg f$. Since $f(x)$ is the polynomial of the least degree that cannot be expressed as a product of irreducible monic polnomials, $r(x)$ and $t(x)$ must be expressible as a product of irreducible monic polynomials. But this would contradict the fact that $f(x)$ is not expressible as a product of irreducible monic polynomials, and so $f(x)$ must be

$$f(x) = l_1(x)l_2(x)\ldots l_m(x)$$

where $l_i(x)$ is an irreducible monic polynomial, for $1 \leq i \leq m$. For the case where $f(x)$ is not monic, say with a as its leading coefficient, we would have

$$f(x) = al_1(x)l_2(x)\ldots l_m(x).$$

For uniqueness, suppose

$$f(x) = cl_1(x)l_2(x)\ldots l_m(x) = dk_1(x)k_2(x)\ldots k_n(x)$$

for units $c, d \in F^*$ and irreducible monic polynomials l_i, k_j for $1 \leq i \leq m$ and $1 \leq j \leq n$. Since $l_1(x) \mid f(x)$, by Proposition 86, $l_1(x) \mid k_j(x)$ for some $1 \leq j \leq n$. Relabelling the indices for the k_j's if necessary, we can have that $l_1(x) \mid k_1(x)$. Since $k_1(x)$ is irreducible and monic, we must have that $l_1(x) = k_1(x)$.

Now if we continue this line of argument for $i = 2, 3, ..., m$, and end up with $l_2(x) = k_2(x)$, $l_3(x) = k_3(x)$, $\ldots$, $l_m(x) = k_m(x)$, where, WLOG, we suppose that $m \leq n$. However, we must have that $n = m$, otherwise we would have some k_j, where $m < j \leq n$ that cannot divide any of the l_i's. $\square$

For the sake of comparison with $\mathbb{Z}$, observe the table below:

	$\mathbb{Z}$	$F[x]$
elements	m	$f(x)$
size	$\lvert m \rvert$	$\deg f$
units	$\{\pm 1\}$ $\left(\mathbb{Z} \setminus \{0\}\right) \big/ \{\pm 1\} \cong \mathbb{N}$	F^* $\left(F[x] \setminus \{0\}\right) \big/ F^* \cong \{h : h \text{ is monic }\}$
unique factorization	$m = \pm 1 p_1^{\alpha_1} \dots p_n^{\alpha_n}$ p_i prime	$f(x) = c l_1(x)^{\alpha_1} \dots l_n(x)^{\alpha_n}$ $\deg f \geq 1$ and l_i are irreducible
ideals	$\langle\, n \,\rangle : n \in \mathbb{N}$ $\mathbb{Z} \big/ \langle\, n \,\rangle$ is a field iff n prime	$\langle\, h(x) \,\rangle : h$ monic $F[x] \big/ \langle\, h(x) \,\rangle$ is a field iff $h(x)$ is irreducible

In the next section, we will be investigating if the analogy given in the last row for polynomials holds.

29.1.2 Quotient Rings of Polynomials

Proposition 88 (Ideals of $F[x]$ are Principal Ideals)

If F is a field. Then all ideas of $F[x]$ are of the form

$$\langle\, h(x) \,\rangle = h(x)F[x] \quad \textit{for any } h(x) \in F[x].$$

If $\langle\, h(x) \,\rangle \neq \{0\}$ and $h(x)$ is monic, then it is uniquely determined.

Proof

Let A be an ideal of $F[x]$. If $A = \{0\}$, then $A = \langle\, 0 \,\rangle$. If $A \neq \{0\}$, then it contains a non-zero polynomial. Since A is an ideal, it has a monic polynomial[2]*. Amongst all monic polynomials in A, choose $h(x) \in A$ that has the minimal degree. Clearly, $\langle\, h(x) \,\rangle \subseteq A$. To prove for $\supseteq$, note that for $f(x) \in A$, by Proposition 84,*

$$\exists q(x), r(x) \in F[x] \quad f(x) = q(x)h(x) + r(x) \quad \deg r < \deg h.$$

If $r(x) \neq 0$, then let $u \neq 0$ be the leading coefficient of $r(x)$. Then since

[2] If $f(x) \in A$ has a leading coefficient a, then we know that $a^{-1} \in F$, and so $a^{-1} f(x) \in F f(x) \subseteq A$ is monic.

A is an ideal and $f(x), h(x) \in A$, we have

$$\begin{aligned} u^{-1}r(x) &= u^{-1}\left(f(x) - q(x)h(x)\right) \\ &= u^{-1}f(x) - u^{-1}q(x)h(x) \in A. \end{aligned}$$

Then we have that $\deg u^{-1}r = \deg r < \deg h$ is a monic polynomial in A, contradicting the minimality of $\deg h$. Thus $r(x) = 0$ and so $f(x) = q(x)h(x) \in \langle\, h(x)\, \rangle$. Therefore $A \langle\, h(x)\, \rangle$ and so $A = \langle\, h(x)\, \rangle$.

Now suppose that $A = \langle\, h(x)\, \rangle = \langle\, k(x)\, \rangle$. Then we must have $h(x) \mid k(x)$ and $k(x) \mid h(x)$. Since $h(x)$ and $k(x)$ are both monic, by Proposition 83, we have that $h(x) = k(x)$. $\square$