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`

30 Lecture 30 Jun 13th 2018

30.1 Polynomial Ring (Continued 3)

30.1.1 Quotient Rings of Polynomials (Continued)

Let A be a non-zero ideal in $F[x]$. By Proposition 88, we know that A is a principal ideal and can be written as $A = \langle\, h(x) \,\rangle$, for a unique polynomial $h(x) \in F[x]$.

Suppose that $\deg h = m \geq 1$. Consider the quotient ring $R = F[x]/A$, and so we have

$$R = \left\{ \overline{f(x)} : f(x) + A, f(x) \in F[x] \right\}.$$

Write $t = \bar{x} = x + A$. Then by the **Division Algorithm**[1], we have

$$R = \{\overline{a_0} + \overline{a_1}t + \ldots + \overline{a_{m-1}}t^{m-1} : a_i \in F\}.$$

[1] This entire part until Proposition 89 might need to be rewritten since I am a little lost as to some of the details regarding the discussion.

The map $\theta : F \to R$, given by $a \mapsto \bar{a}$, is an injective homomorphism, since θ is not a zero map and $\ker\theta$ is an ideal of F Note that a field F has only 2 ideals: $\{0\}$ and F itself. Since $\ker\theta \neq F$, we have that $\ker\theta = \{0\}$ and so θ is injective.. Since we have $F \cong \theta(F)$ by the First Isomorphism Theorem for Rings, by identifying F with $\theta(F)$, we can write

$$R = \{a_0 + a_1t + \ldots a_{m-1}t^{m-1} : a_i \in F\}.$$

It is clear that, in R, we have

$$\begin{gathered} a_0 + a_1t + \ldots + a_{m-1}t^{m-1} = b_0 + b_1t + \ldots + b_{m-1}t^{m-1} \\ \iff \\ \forall i \in \mathbb{Z}\ 0 \leq i \leq m-1 \quad a_i = b_i \end{gathered}$$

Finally, in the ring R, we have $h(t) = 0$.

The following proposition follows from the above discussion.

Proposition 89

Let F be a field and let $h(x), f(x) \in F[x]$ be monic with $(\deg h, \deg f \geq 1)$. Then the quotient ring $R = F[x]/A$ is given by

$$R = \{a_0 + a_1 t + \ldots + a_{m-1} t^{m-1} : a_i \in F,\ h(t) = 0\}$$

in which each element of R can be uniquely represented in the above form.

Note

In $\mathbb{Z}$, we have that $\mathbb{Z}/\langle\ n\ \rangle = \mathbb{Z}_n = \{[0], [1], ..., [n-1]\}$ which is analogous to our statement in Proposition 89 for the case of integers.

Example 30.1.1

Consider $\mathbb{R}[x]$ and let $h(x) = x^2 + 1 \in \mathbb{R}[x]$. Then

$$\mathbb{R}[x] = \{a + bt : a, b \in \mathbb{R},\ t^2 + 1 = 0\} \cong \{a + bi : a, b \in \mathbb{R},\ i^2 = -1\} = \mathbb{C}$$

Note

Recall that $\mathbb{Z}_n$ is a field (or an integral domain) if and only if n is prime.

Proposition 90

Let F be a field nad $h(x) \in F[x]$ be a monic polynomial with $\deg h \geq 1$. TFAE:

1. *$F[x]/\langle\ h(x)\ \rangle$ is a field;*
2. *$F[x]/\langle\ h(x)\ \rangle$ is an integral domain;*
3. *$h(x)$ is irreducible in $F[x]$.*

Proof

(1) $\implies$ (2) *since a field is an integral domain (see Proposition 74).*

(2) $\implies$ (3)*: Write* $A = \langle\, h(x) \,\rangle$*, If* $h(x) = f(x)g(x)$ *for* $f(x), g(x) \in F[x]$*, then*

$$\begin{aligned}[f(x) + A][g(x) + A] &= f(x)g(x) + A \quad \because A \text{ is an ideal} \\ &= h(x) + A = 0 \in F[x]/A.\end{aligned}$$

Then by (2)*, either* $f(x) + A = 0$ *or* $g(x) + A = 0$*, i.e. either* $f(x) \in A$ *or* $g(x) \in A$*. But if* $f(x) \in A = \langle\, h(x) \,\rangle$*, then* $f(x) = q(x)h(x)$ *for some* $q(x) \in F[x]$*. Then* $h(x) = f(x)g(x) = q(x)h(x)g(x)$*, which then implies that* $0 = h(x)[1 - q(x)g(x)] \implies q(x)g(x) = 1$ *since* $F[x]$ *is an integral domain. Then we have that* $\deg g = 0$*. Similarly, if* $g(x) \in A$*, then we have* $\deg f = 0$*. Therefore,* $h(x)$ *is irreducible in* $F[x]$ *by definition.*

(3) $\implies$ (1)*: Note that* $F[x]/\langle\, h(x) \,\rangle$ *is a commutative ring. To show that it is a field, it suffices to show that every non-zero element of* $F[x]/\langle\, h(x) \,\rangle$ *has an inverse. Let* $f(x) + A \neq 0 \in F[x]/\langle\, h(x) \,\rangle$ *with* $f(x) \in F[x]$*. Then* $f(x) \notin A$*, and so* $h(x) \nmid f(x)$*. Since* $h(x)$ *is irreducible by* (3)*, we have that*

$$d(x) = \gcd[f(x), h(x)] = 1.$$

Then by Proposition 85, $\exists u(x), v(x) \in F[x]$ *such that*

$$1 = u(x)h(x) + v(x)f(x).$$

Since $h(x)u(x) \in A$*, we have that*

$$[v(x) + A][f(x) + A] = 1 + A.$$

It follows that $f(x) + A$ *has an inverse in* $F[x]/\langle\, h(x) \,\rangle$ *and thus* $F[x]/\langle\, h(x) \,\rangle$ *is a field.* □

30.2.1 Irreducibles and Primes

We have discussed much about the similarities between $\mathbb{Z}$ and $F[x]$, and in this chapter, we wish to abstract these similarties and study them in a more general manner to see if other sets that share the same kind of properties. For example, if a set has a **unique factorization** for elements and the **principal ideal** being the only ideal of the set, then do we still see the same analogy playing out?

Definition 52 (Division)

Let R be an integral domain and $a, b \in R$. We say that $a \mid b$ if $b = ca$ for some $c \in R$.

Note

Recall that in $\mathbb{Z}$, if $n \mid m$ and $m \mid n$, then $n = \pm m$, and the ideal generated by them are the same, i.e. $\langle\, n \,\rangle = \langle\, m \,\rangle$.

Similarly so in $F[x]<$ if $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $f(x) = cg(x)$ for some $x \in F[x]^* = F^*$, and $\langle\, f(x) \,\rangle = \langle\, g(x) \,\rangle$.

Proposition 91 (Division in an Integral Domain)

Let R be an integral domain. Then $\forall a, b \in R$, TFAE:

1. *$a \mid b$ and $b \mid a$;*
2. *$a = ub$ for some unit $u \in R$;*
3. *$\langle\, a \,\rangle = \langle\, b \,\rangle$.*

This should be an easy exercise.

Exercise 30.2.1
Prove Proposition 91.

Definition 53 (Association)

*Let R be an integral domain. $\forall a, b \in R$, we say that a is **associated to** b, denoted by $a \sim b$, if $a \mid b$ and $b \mid a$.*

Note

By Proposition 91, we have that $a \sim a$ for any $a \in R$.

Also, $a \sim b \iff b \sim a$.

We also have $a \sim b \land b \sim c \implies a \sim c$.

In other words, $\sim$ is an equivalence relation in R. Also, it can be shown that[2]

1. $a \sim a' \land b \sim b' \implies ab \sim a'b'$.
2. $a \sim a' \land b \sim b' \implies (a \mid b \iff b \mid a)$

[2] More exercise is always good.

Exercise 30.2.2
Prove that the two statements following this is true.

Example 30.2.1

Let $R = \mathbb{Z}[\sqrt{3}] = \{m + n\sqrt{3} : m, n \in \mathbb{Z}\}$. Note that this is an integral domain[3]*. Observe that*

$$(2+\sqrt{3})(2-\sqrt{3}) = 1 \implies 2+\sqrt{3} \text{ is a unit in } R.$$

Then we would have

$$3 + 2\sqrt{3} = (2+\sqrt{3})\sqrt{3}$$

and so by Proposition 91, we have

$$3 + 2\sqrt{3} \sim \sqrt{3} \in \mathbb{Z}[\sqrt{3}].$$

[3] For $(a+b\sqrt{3}), (c+d\sqrt{3}) \in R$ such that

$$(a+b\sqrt{3})(c+d\sqrt{3}) = 0$$

we would have that

$$(a+b\sqrt{3})(a-b\sqrt{3})(c+d\sqrt{3})(c-d\sqrt{3}) = 0$$
$$(a^2-3b^2)(c^2-3d^2) = 0.$$

Since $\mathbb{Z}$ is an integral domain, suppose $a^2 - 3b^2 = 0$. If $b = 0$, then $a = 0$ and we are done. If $b \neq 0$, then we have $3 = \left(\frac{a}{b}\right)^2$, and we notice that $\sqrt{3}$ is irrational. Thus it can only be that $b = 0$. Therefore, $a + b\sqrt{3} = 0$, implying that there are no zero divisors in $R = \mathbb{Z}[\sqrt{3}]$.