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`

31 Lecture 31 Jul 16th 2018

31.1 Factorizations in Integral Domains (Continued)

31.1.1 Irreducibles and Primes (Continued)

Note

Recall that if R is an integral domain and $a, b \in R$, we say that $a \mid b$ if $\exists c \in R$ such that $b = ca$.

Also, recall the definition of **associativity**.

Definition (Associativity)

If $a \mid b$ and $b \mid a$, then we say that a is associative to b, and denote $a \sim b$ if and only if $\exists u \in R$, which is a unit, such that $a = ub$, and we have $\langle\, a \,\rangle = \langle\, b \,\rangle$.

Definition 54 (Irreducible)

*Let R be an integral domain. We say $p \in R$ is **irreducible** if $p \neq 0$ is not a unit, and $p = ab \in R$, then either a or b is a unit. An element that is not **irreducible** is **reducible**.*

Example 31.1.1

Let $R = \mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} : m, n \in \mathbb{Z}\}$ and $p = 1 + \sqrt{-5}$. We want to show that p is an irreducible in R. Note that for $z = m + n\sqrt{-5} \in$

R, the **norm** *of z is defined to be*

$$N(z) = \left(m + n\sqrt{-5}\right)\left(m - n\sqrt{-5}\right) = m^2 + 5n^2 \in \mathbb{N} \cup \{0\}$$

Note that[1]

$$N(xy) = N(x)N(y).$$

Now suppose that $p = ab \in R$. *Then*

$$6 = N(p) = N(a)N(b).$$

However, since $N(z) = m^2 + 5n^2$ *for some* $m, n \in \mathbb{Z}$, *we must have that* $N(z) \neq 2, 3$. *Thus, we have either* $N(a) = 1$ *or* $N(b) = 1$, *which in turn implies that* $a = \pm 1$ *and* $b = \pm 1$, *which implies that a or b is a unit. Therefore, p is irreducible.*

[1] **Proof**
Let $x = m + n\sqrt{-5}$ *and* $y = a + b\sqrt{-5}$. *Note that*

$$N(x) = m^2 + 5n^2.$$

Then

$$\begin{aligned} &N(x)N(b) \\ &= m^2a^2 + 25n^2b^2 + 5(n^2a^2 + m^2b^2). \end{aligned}$$

and since

$$xy = ma - 5nb + \sqrt{-5}(na + mb),$$

we have

$$\begin{aligned} &N(xy) \\ &= (ma - 5nb)^2 + 5(na + mb)^2 \\ &= m^2a^2 + 25n^2b^2 + 5(n^2a^2 + m^2b^2) \end{aligned}$$

Proposition 92 (Properties of Irreducibles)

Let R be an integral domain. Let $0 \neq p \in R$. *TFAE:*

1. *p is irreducible;*
2. $d \mid p \implies d \sim 1 \veebar d \sim p$;
3. $p \sim ab \in R \implies p \sim a \veebar p \sim b$;
4. $p = ab \in R \implies p \sim a \veebar p \sim b$.

Consequently, if $p \sim q$, *we have p is irreducible if and only if q is irreducible.*

Proof

(1) $\implies$ (2): $\quad d \mid p \implies \exists c \in R \quad dc = p$.

d is a unit $\implies d \sim 1 \ \square$;

d is not a unit $\implies$ *c is a unit* $\because$ *p is irreducible*

$\implies \exists c^{-1} \in R \quad cc^{-1} = 1 \implies d = pc^{-1} \implies d \sim p$.

(2) $\implies$ (3) : $\quad p \sim ab \implies \exists c, c^{-1} \in R \ \ cc^{-1} = 1 \quad p = cab$

Suppose $p \not\sim a$.

$a \mid cab \implies a \mid p \overset{(2)}{\implies} a \sim 1 \implies$ *ca is a unit* $\implies p \sim b$.

(3) $\implies$ (4) : $\quad$ 1 *is a unit and so* $p = ab \implies p \sim ab$, *and the result follows from* (3).

$(4) \implies (1)$: $\because (4)\ \ p = ab \implies p \sim a \veebar p \sim b$.

WLOG $p \sim a \implies \exists c, c^{-1} \in R\ \ cc^{-1} = 1 \quad p = ac \implies ac = ab$

Note $a \neq 0 \because p \neq 0 \land p \sim a$.

Then by Proposition 73, $c = b \implies b$ *is a unit* $\implies p$ *is irreducible.*

By (3) *and* (1), $p \sim q \iff p, q$ *are irreducibles.* ☐

Definition 55 (Prime)

Let R *be an integral domain and* $p \in R$. *We say* p *is* ***prime*** *in* R *if* $p \neq 0$ *is not a unit, and if* $p \mid ab \in R \implies p \mid a \veebar p \mid b$.

Note

If $p \sim q$, *then* p *is prime* $\iff q$ *is prime. This is a clear result, since* $p \sim q \implies p \mid q \land q \mid p$, *and if* p *is prime, then* $q \mid p \mid ab \implies q \mid p \mid a \veebar q \mid p \mid b$.

Also, by induction, if p *is prime and*

$$p \mid a_1 a_2 \ldots, a_n,$$

then $p \mid a_i$ *for some* $1 \leq i \leq n$.

Proposition 93 (Primes are Irreducible)

Let R *be an integral domain and* $p \in R$. p *is prime* $\implies p$ *is irreducible.*

Proof

$\because p$ *is prime* $\quad p = ab \implies p \mid a \veebar p \mid b$.

WLOG $p \mid a \implies \exists d \in R \quad dp = a$

$\implies a = dp = dab = adb \quad \because R$ *is commutative*

$\because a \neq 0$ *and* R *is an integral domain, by Proposition 73,* $1 = db \implies b$ *is a unit (with* d *being its multiplicative inverse).*

$\therefore p$ *is irreducible.* ☐

The converse of Proposition 93 is false.

Example 31.1.2

Recall from Example 31.1.1 that $1+\sqrt{-5}$ *is irredubile in* $\mathbb{Z}[\sqrt{-5}]$. *Recall that for* $d = m + n\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, *we defined the* ***norm*** *as*

$$N(d) = m^2 + 5n^2 \in \mathbb{N} \cup \{0\}.$$

Before proceeding further, note that

$$2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5}) = p(1-\sqrt{-5}).$$

Suppose p *is prime, which then* $p \mid 2 \cdot 3 \implies p \mid 2 \veebar p \mid 3$. *Suppose* $p \mid 2 \implies \exists q \in \mathbb{Z}[\sqrt{-5}] \quad 2 = pq$. *It follows that*

$$4 = N(2) = N(p)N(q) = 6N(q)$$

which is impossible. Similarly, $p \mid 3 \implies \exists r \in R \quad 3 = rp \implies$

$$9 = N(3) = N(r)N(p) = 6N(r)$$

is also impossible. Therefore, p *is not prime.*

31.1.2 Ascending Chain Condition

Definition 56 (Ascengding Chain Condition on Principal Ideals (ACCP))

An integral domain R *is said to satisfy the* ***ascending chain condition on principal ideals*** *(ACCP) if for any ascending chain*

$$\langle\, a_1 \,\rangle \subseteq \langle\, a_2 \,\rangle \subseteq \langle\, a_3 \,\rangle \subseteq \ldots$$

of principal ideals in R, $\exists n \in \mathbb{N}$ *such that*

$$\langle\, a_n \,\rangle = \langle\, a_{n+1} \,\rangle = \ldots\,.$$

Example 31.1.3

$\mathbb{Z}$ *satisfies ACCP.*

If $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \ldots$ *in* $\mathbb{Z}$*, then*

$$a_2 \mid a_1,\ a_3 \mid a_2,\ \ldots\ .$$

Taking the absolute value of each of the a_i*'s, we have that*

$$|a_1| \geq |a_2| \geq |a_3| \geq \ldots\ .$$

Since each of the $|a_i| \geq 0$ *is an integer, there must be some* $n \in \mathbb{N}$ *where*

$$|a_n| = |a_{n+1}| = \ldots\ .$$

This implies that $a_{i+1} = \pm a_i$ *for* $i \geq n$*. Therefore, we have that*

$$\langle a_i \rangle = \langle a_{i+1} \rangle \quad \text{for } i \geq n,$$

thus showing that the ACCP is satisfied.

Theorem 94 (Factorization on an Integral Domain Satisfying ACCP)

Let R *be an integral domain that satisfies ACCP. Let* $0 \neq a \in R$ *be a non-unit. Then* a *is a product of irreducible elements of* R*.*

Proof

Suppose to the contrary that a *is not a product of irreducible elements of* R*. Then* a *itself must not be irreducible. By Proposition 92,* $\exists x_1 \in R$ *such that*

$$a = x_1 a_1 \quad a \not\sim x_1 \wedge a \not\sim a_1.$$

Note that at least one of x_1 *or* a_1 *is not a product of irreducible elements, for otherwise* a *would be a product of irreducible elements. WLOG, suppose* a_1 *is not a product of irreducible elements. Then Proposition 92* $\implies \exists x_2 \in R$

$$a_1 = x_2 a_2 \quad a_1 \not\sim x_2 \wedge a \not\sim a_2.$$

We can continue this argument infinitely so, in which we will then get an ascending chain of principal ideals

$$\langle a \rangle \subseteq \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \ldots\ .$$

However, since

$$a \not\sim a_1 \not\sim a_2 \not\sim \ldots ,$$

🔥 *Proposition 91 implies that*

$$\langle\, a \,\rangle \subsetneq \langle\, a_1 \,\rangle \subsetneq \langle\, a_2 \,\rangle \subsetneq \ldots ,$$

which contradicts the assumption that R satisfies ACCP. Therefore, all non-unit $0 \neq a \in R$ is a product of irreducible elements of R. $\square$