Note for PID/UFD

Date: May 21 Made by Eric

0. Notation

Definition 1. *We call a commutative ring with unity that have no zero-divisor an integral domain D*

Definition 2. *Suppose $x, y \in D$. Then*

$$x|y \implies \exists z \in D, y = xz \tag{1}$$

1. Associations Class

1.1 Definition of Associate and Association Class

Lemma 1. *For all integral domain D, we can partition the elements of D into equivalence classes by means of gathering two elements into the same class if they are **associate**, that is, there exists an unit that can multiply one of them, thus becoming the other.*

Proof. Observe

$$a = 1a \tag{2}$$

$$b = au \implies a = bu^{-1} \tag{3}$$

$$b = au, c = bu_1 \implies c = auu_1 \tag{4}$$

■

Definition 3. *Elements a, b of an integral domain D are **associate** in D if there exists unit d such that $b = ad$, and the equivalent class given by association is called **association class**, and written by $[x]$ if it contain x.*

Lemma 2.

$$a \text{ and } b \text{ are associate} \iff a|b \text{ and } b|a \tag{5}$$

Proof. Suppose $b = au$. Observe $a = bu^{-1}$, and we see $a|b$ and $b|a$. Suppose $b = ax$ and $a = by$. Observe $ab = abxy \implies xy = 1 \implies x$ and y are units $\implies a$ and b are associate. ■

1.2 Structure of Association Class

Lemma 3. *Suppose u is an unit.*

$$[u] \text{ contains all units.}$$

Proof. Suppose a, b are units. Observe

$$b = a(a^{-1}b) \tag{6}$$

where

$$(a^{-1}b)^{-1} = ab^{-1} \tag{7}$$

imply that $a^{-1}b$ is a unit. ■

Lemma 4. *We can "well-define" multiplication on the set of all association classes by means of*

$$[x_1][x_2]\cdots[x_n] = [x_1\cdots x_n] \tag{8}$$

Proof. Suppose $x_i' = u_i x_i$. Observe

$$x_1'\cdots x_n' = (u_1\cdots u_n)(x_1\cdots x_n) \in [x_1\cdots x_n] \tag{9}$$

■

Corollary 4.1.

$$[u][x] = [x] \tag{10}$$

Corollary 4.2.

$$[a] = [x_1]\cdots[x_n] \iff a = ux_1\cdots x_n \textit{ for some unit } u \tag{11}$$

Proof. $(\longleftarrow)$

$$[a] = [u][x_1]\cdots[x_n] = [x_1]\cdots[x_n] \tag{12}$$

$(\longrightarrow)$

$$[a] = [x_1]\cdots[x_n] \implies a \in [x_1\cdots x_n] \implies a = ux_1\cdots x_n \text{ for some unit } u \tag{13}$$

■

Definition 4. *Suppose $x, y \in D$. Then*

$$[x]|[y] \iff \exists z \in D, [y] = [x][z] \tag{14}$$

Corollary 4.3.

$$p|a \iff [p]|[a] \tag{15}$$

Proof. From left to right is obvious. From right to left , Observe $[p]|[a] \implies \exists z \in D, pz = ua \implies u^{-1}pz = a \implies p|a$. ■

Lemma 5. *Suppose u is a unit. Then*

$$[u] = [x][y] \iff [x] = [u] = [y] \tag{16}$$

Proof. From right to left is obvious. From left to right, we arbitrarily pick $u_1 = x_1y_1$, and observe

$$x_1(y_1u_1^{-1}) = 1 = y_1(x_1u_1^{-1}) \tag{17}$$

■

2. Irreducibles and Primes

2.1 Definition of Irreducibles and Primes

Definition 5. *An non-zero non-unit element p is an **irreducible** if*

for all expression $p = cd$, that c or d is a unit.

Definition 6. *A non-zero non-unit element p is an **prime** if $p|ab \implies p|a$ or $p|b$*

2.2 Inner Structure of Irreducibles and Primes

Lemma 6. *All irreducibles form some association class**es**.*

Proof. Suppose p is an irredubile and u is an unit. Arbitrarily factorize pu in the form $pu = mn$. We see $p = (u^{-1}m)n$. Suppose n is not a unit, then by the definition of irreducibility of p, we know $u^{-1}m$ is a unit u_c, then $m = uu_c$ is a unit. In conclusion, either m or n is a unit. Then we have deduced pu is irreducible. ■

Lemma 7. *All primes form some association class**es**.*

Proof. Suppose p is a prime and u is an unit, and suppose $pu|cd$. Because $p|u^{-1}cd$, we know $p|u^{-1}c$ or $p|d$, if $p|u^{-1}c$ is true, then $pu|c$ finish our proof. If $p|d$, then we express d in the form $d = px$ and see $d = (pu)u^{-1}x$, which implies $pu|d$. ■

Definition 7. *The association class containing irreducible/prime is called a **irreducible/prime association class**.*

2.3 Outer Structure of Irreducibles and Primes*

Lemma 8. *The set of prime association class are a subset of the set of irreducible association classes.*

Proof. Suppose p is a prime and arbitrarily factorize p in the form $p = cd$.

$$p = cd \implies p|cd \implies p|c \text{ or } p|d \tag{18}$$

WOLG, suppose $p|c$, and express c in the form $c = px$

Then we see $p = cd = p(xd)$, which implies $xd = 1$, then d is a unit. ■

3. Existence and Uniqueness of Factorization

3.1 Definition of Existence and Uniqueness of Factorization

Definition 8. *An integral domain D satisfy the property **"existence of factorization"** if*

*For all non-zero non-unit element $a \in D$ we can factorize a in some **completely reduced** form*

$$a = up_1p_2 \cdots p_n \tag{19}$$

where p_i are irreducibles and u is a unit.

*Also we call such integral domain D an **atomic domain**.*

Corollary 8.1. *For all non-zero non-unit association class $[a]$ in an atomic domain D, we can facatorize $[a]$ in some completely reduced form*

$$[a] = [p_1] \cdots [p_n] \tag{20}$$

Definition 9. *An integral domain D is **unique factorization domain**, UFD, if D it satisfy "existence of factorization" and it satisfy "**uniqueness of factorization**"; that is*

Any two factorization of a

$$a = up_1p_2 \cdots p_n \text{ and } a = u'p_1'p_2' \cdots p_m' \tag{21}$$

are "only switch of order and of pick of element from irreducible association class", that means $n = m$ and we can switch the order of $(p_1', \ldots, p_n')$ to some order $(p_{N(1)}', \ldots, p_{N(n)}')$ so that $[p_i] = [p_{N(i)}']$

Corollary 8.2. *Suppose D is an UFD, then the **factorization** $[a] = [p_1] \cdots [p_n]$ is unique.*

3.2 Factorize elements of UFD into completely reduced from

Lemma 9. *Suppose D is an UFD, $p \in D$ is an irreducible. Then*

$$p|a \iff [p]|[a] \iff [p] \text{ appears in the factorization of } [a]$$

Lemma 10. *If D is UFD, then the set of irreducible association classes and the set of prime association classes are the same.*

Proof. Lemma 8 states that in all integral domain, a prime must be an irreducible. We only have to show in UFD, an irreducible must also be a prime.

Let p be an irreducible and suppose $p|ab$. By the "existence of factorization" and Lemma 9, we can express $[ab]$ in the form

$$[ab] = [p][p_1] \cdots [p_n] \tag{22}$$

Factorize $[a]$ and $[b]$ in the form

$$[a] = [p_{a_1}] \cdots [p_{a_m}] \text{ and } [p_{b_1}] \cdots [p_{b_{n-m}}] \tag{23}$$

We see

$$[p][p_1] \cdots [p_n] = [ab] = [a][b] = [p_{a_1}] \cdots [p_{a_m}][p_{b_1}] \cdots [p_{b_{n-m}}] \tag{24}$$

Because the factorization is unique, we know $[p] = [p_{a_i}]$ or $[p_{b_i}]$ for some i; that is $[p]$ appears in the factorization of $[a]$ or $[b]$, which indicate that $p|a$ or $p|b$.

■

4. PID is UFD

4.1 Definition of PID

Definition 10. *An integral domain D is* ***principal ideal domain,*** *PID, if D satisfy*

Every ideal N is generated by some element a, that is

$$N = \langle a \rangle = \{ax | x \in D\} \tag{25}$$

4.2 PID satisfy "existence of factorization"

Lemma 11. *Suppose $N_1 \subset N_2 \subset \cdots$ be an ascending chain of ideals N_i in D. Then $N = \bigcup N_i$ is an ideal of D.*

Proof. Arbitrarily pick a, b from N and c from D, and WOLG, suppose $a \in N_j$ and $b \in N_k$ and $j \leq k$.

$$a \in N_j \subseteq N_k \implies a + b \in N_k \subseteq N \tag{26}$$

$$ac \in N_i \implies ac \in N \tag{27}$$

■

Lemma 12. *Suppose D is a PID and $N_1 \subset N_2 \subset \cdots$ is an ascending chain of ideals N_i in D. Then the ascending chain N_i must be finite.*

Proof. Suppose $N = \bigcup N_i = \langle c \rangle$ and suppose $c \in N_r$.

Assume $\exists N_{r+1}, x \in N_{r+1} \setminus N_r$

$$x \in N_{r+1} \subseteq N = \langle c \rangle \implies x = cd, \exists d \in D \implies x \in N_r \text{ CaC} \tag{28}$$

■

Lemma 13.

$$\langle a \rangle \subseteq \langle b \rangle \iff b | a \tag{29}$$

Proof. Express a in the form $a = bd$. Arbitrarily pick x from $\langle a \rangle$ and express x in the form $x = ac$, then we see $x = bdc \implies x \in \langle b \rangle$. For another direction, observe $a \in \langle b \rangle$ ■

Corollary 13.1.

$$\langle a \rangle = \langle b \rangle \iff a | b \text{ and } b | a \iff a, b \text{ are associate} \tag{30}$$

Theorem 14. ***(Existence of Factorization for PID)*** *Suppose D is an PID. Then*

All non-zero and non-unit element a can be expressed as a finite product of irreducibles p_i

Proof. Our goal here is simple, we find an algorithm to faztorize a into a finite product of irreducibles. We first try to find an irreducible that divides x with the following algorithm.

"Find **one** factor Algorithm (input: x)"

Step 0: Let $x_0 = x$ and $i = -1$.

Step 1: Let i increase by 1. Test if x_i is irreducible. If it is, terminate and output x_i, if not, go to step 2.

Step 2: Because x_i is reducible, we can express x_i in the form $x_i = x_{i+1}y_{i+1}$ for some non-units x_{i+1}, y_{i+1}. Repeat step 1.

We now show that this algorithm terminate eventually, and the output is an irreducible factor of the input x.

Assume the algorithm never terminate.

Then there exists a sequence of $\{x_i\}$ of infinite length, where $x_{i+1}y_{i+1} = x_i$ and y_{i+1} are non-unit.

We know $x_i \not| x_{i+1}$ because if $x_i | x_{i+1}$, then y_{i+1} is a unit. Then by Lemma 13, we know $\langle x_i \rangle \subset \langle x_{i+1} \rangle$. So, we know there is an ascending chain $\langle x_0 \rangle \subset \langle x_1 \rangle \subset \cdots$ of infinite length, which CaC to Lemma 12.

Suppose the output is x_m. Obviously, x_m is irreducible, and we see

$$x_m | x_{m-1} \text{ and } x_{m-1} | x_{m-2} \text{ and } \cdots \text{ and } x_1 | x_0 = x \text{ (done)} \tag{31}$$

Now we try to completely reduce x with another algorithm.

"Completely Reducing Algorithm (input: x)"

Step 0: Let $x_0 = x$ and $i = -1$.

Step 1: Let i increase by 1. Operate "Find **one** factor Algorithm" with input x_i, and obtain the output y_i, and express $x_i = x_{i+1}y_i$

Step 2: Test if $\Pi_{j=0}^{i} y_j = x$. If true, output $\Pi_{j=0}^{i} y_j$ and terminate. If not, go to Step 1.

We now show that this algorithm terminate eventually, and obviously if it does, it output a finite product of irreducibles that is x.

Assume the algorithm never terminate.

Then there exists a sequence $\{x_i\}$ of infinite length, where $x_i = x_{i+1}y_i$, which indicate $x_{i+1} | x_i$

Because y_i is irreducible, so it is non-unit. Then by Lemma 13, we know $\langle x_i \rangle \subset \langle x_{i+1} \rangle$. So, we know there is an ascending chain $\langle x_0 \rangle \subset \langle x_1 \rangle \subset \cdots$ of infinite length, which CaC to Lemma 12. (done) ■

4.3 PID satisfy "uniqueness of factorization"

Lemma 15. *In PID, an ideal $\langle p \rangle$ is maximal if and only if p is irreducible.*

Proof. $(\longrightarrow)$

Assume p is reducible and express p in the form $p = cd$ where c, d are non-unit. $\langle c \rangle$ are proper because c is non-unit, and because d is non-unit, we know $p \not| c$. Then by $c|p$ and Lemma 13, we know $\langle p \rangle \subset \langle c \rangle \subset D$ CaC

$(\longleftarrow)$

Assume $\langle p \rangle$ is not maximal, that is there exists $\langle p \rangle \subset \langle c \rangle \subset D$. Then by Lemma 13, we know $c|p$. Express p in the form $p = cd$. We know c is a non-unit because $\langle c \rangle \subset D$. We deduce d is a non-unit, since if d is a unit, then $c = pd^{-1}$, which indicate $p|c$, which further indicate, by Lemma 13, $\langle p \rangle = \langle c \rangle$. If c, d are both non-unit, then we see $p = cd$ are reducible. CaC

■

Lemma 16. *In PID, the set of irreducible association classes and the set of prime association classes are the same.*

Proof. Lemma 8 states that in all integral domain, a prime must be an irreducible. We only have to show in PID, an irreducible must also be a prime.

Suppose p is an irreducible, and suppose $p|ab$. Notice that $\langle p \rangle$ is a maximal ideal, so it is a prime ideal, and notice $ab \in \langle p \rangle$, so we know either $a \in \langle p \rangle$ or $b \in \langle p \rangle$. In other words, either $p|a$ or $p|b$. ■

Corollary 16.1.

$$p|a_1 \cdots a_n \implies \exists a_i, p|a_i \tag{32}$$

Theorem 17. ***(Uniqueness of Factorization for PID)*** *Suppose D is an PID. Then*

All any two factorization of a

$$up_1p_2 \cdots p_n = a = u'p'_1p'_2 \cdots p'_m \tag{33}$$

are "only switch of order and of pick of element from irreducible association class", that means $n = m$ and we can "switch the order" of p_i so that each of their counterparts are in the same irreducible association class. More precisely, that is

$$\exists\ \textbf{\textit{(bijective)}}\ N : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}, \forall 1 \leq i \leq n, [p_i] = [p'_{N(i)}]$$

Proof. We know $p_1|a = (u')(p'_1 \cdots p'_m)$, and by Lemma 5, we know it will never happens that $p_1|u'$, so we can deduce $p_1|p'_1 \cdots p'_m$, and deduce $p_1|p'_i$ for some p'_i.

Factorize $[p'_i]$ and assume that the output contain more than one irreducible association class. That is, $[p'_i] = [p_j][p_k]$.

Observe $\exists u, p'_i = (up_j)p_k$, and we immediately draw our contradiction. CaC

So we know the factorization of $[p'_i]$ is $[p'_i]$ and we know by $p_1|p'_i$ that $[p_1]$ takes part in the factorization of $[p'_i]$. Then we can deduce $[p_1] = [p'_i]$. So, we define $N(1) = i$, and observe that $[p_1] = [p'_i] = [p'_{N(1)}]$.

Express $p'_{N(1)}$ in the form $p'_{N(1)} = u_1p_1$ for some unit u_1, and express a in the form

$$up_1p_2p_3 \cdots p_n = a = u'(u_1p_1)p'_1 \cdots p'_m \tag{34}$$

By Cancellation Law in Integral domain, we see

$$up_2p_3 \cdots p_n = (u'u_1)p'_1 \cdots p'_m \tag{35}$$

Where $p'_{N(1)}$ is not in the RHS of the equation. Notice $p_2|(u'u_1)p'_1 \cdots p'_m$, and repeat what we do to complete the proof. Notice that if $m < n$ or $n < m$, we will run into the situation of $\Pi p_i = 1$. ■

5. $D[x]$ is UFD if D is UFD

5.0 Definition of primitive polynomial and content

Lemma 18. *Suppose D is UFD, and $\{[x_i]\}$ is finite. Then*

There exists a unique greatest element $[d_m]$ in the set $S := \{[d] | \forall i, [d]$ divides $[x_i]\}$, as we define greatest by $\forall [d] \in S, [d]$ divides $[d_m]$

Proof. We first prove the existence of the greatest element in S by explicitly giving one.

Because D is UFD, and $\{[x_i]\}$ is finite, we can express every element $[x_c] \in \{[x_i]\}$ in the form $[x_c] = \Pi_{j=1}^n [p_j]^{e_j^c}$ for fixed values n and $e_j^c \in \mathbb{Z}_0^+$. Observe that $[d_m] := \Pi_{j=1}^n [p_j]^{e_j^m}$ where e_j^m is given by $min(\{e_j^i\})$, satisfy $\forall i, [d_m]|[x_i]$, since $\forall i, \forall 1 \leq j \leq n, e_j^m \leq e_j^i$; in other words, $[d_m] \in S$. **(Exactly the same concept of finding gcd in natural number with primes)**

To see that $[d_m]$ is "a" greatest element. Arbitrarily pick $[d_r]$ from S, and express $[d_r]$ in the form $[d_r] = \Pi_{j=1}^n [p_j]^{e_j^r}$, to observe

$$\forall i, [d_r] \text{ divides } [x_i] \implies \forall i, \forall 1 \leq j \leq n, e_j^r \leq e_j^i \tag{36}$$

$$\implies \forall 1 \leq j \leq n, e_j^r < min(\{e_j^i\}) = e_j^m \implies [d_r]|[d_m] \text{ (done)} \tag{37}$$

To see that $[d_m]$ is unique, assume that there exists another distinct maximal element $[d_{m'}]$, and observe

$$[d_m]|[d_{m'}] \text{ and } [d_{m'}]|[d_m] \implies \exists(y,z) \in D^2, [d_{m'}] = [d_m][y], [d_m] = [d_{m'}][z] \quad (38)$$

$$\implies [d'_m d_m] = [d'_m d_m][y][z] \implies [y][z] = [u] \quad (39)$$

$$\implies [y] = [u] \implies [d_m] = [d_{m'}] \text{ CaC (done)} \quad (40)$$

■

Definition 11.

$$gcd(\{[x_i]\}) := [d_m] \quad (41)$$

Definition 12. *Suppose D is UFD, and suppose $f(x) = c_n x^n + \cdots + c_1 x_1 + c_0 \in D[x]$. The **contents** of $f(x)$ is $gcd(\{[c_i]\})$ and $f(x)$ is a **primitive polynomial** if*

$$gcd(\{[c_i]\}) = [u] \quad (42)$$

Theorem 19. *That a non-constant polynomial $f(x) \in D[x]$ is irreducible is possible only if it is $f(x)$ primitive.*

Proof. Suppose $f(x) = c_n x^n + \cdots + c_0$ is not primitive, that is $\exists[p], \forall c_i, [p]|[c_i]$. In other word, $f(x) = p(d_n x^n + \cdots + d_0)$, where $c_i = pd_i$. Because p and $d_n x^n + \cdots + d_0$ are non-units, we have deduced $f(x)$ is reducible. ■

5.1 The HARD Ass proof of $D[x]$ being UFD

Lemma 20. *Suppose D is a UFD, and $f(x) = a_0 + a_1 x + \cdots + a_n x^n, g_(x) = b_0 + b_1 x + \cdots b_m x^m \in D[x]$. Then*

$$f(x) \text{ and } g(x) \text{ are primitive} \implies fg(x) \text{ is primitive} \quad (43)$$

Proof. Express $fg(x)$ in the form $fg(x) = \sum_{i=1}^{n+m} c_0 x^i$, and observe

$$gcd(\{[c_i]\}) = [u] \iff \text{no irreducible } p \text{ divides all } c_0, \ldots, c_{n+m}$$

So we only have to prove the latter.

Arbitrarily pick irreducible p and pick r, s that satisfy

$$p \not| a_r \text{ and } \forall 0 \leq i < r, p|a_i \text{ and } p \not| b_s \text{ and } \forall 0 \leq i < s, p|b_i \quad (44)$$

Notice that we can pick r, s because by premise, $gcd(\{[a_i]\}) = [u] = gcd(\{[b_i]\})$, so no irreducible p can divide all a_i (and b_i). **(Do an experiment of case of $[p]$ does not appear in any factorization of $[a_i]$ and see what is going on. Try to deduce that $[a_r]$ is the first coeffciecnt counting from 0 to n of which $[p]$ does not appear in the factorization.)**

Observe

$$c_{r+s} = (a_0 b_{r+s} + \cdots + a_{r-1} b_{s+1}) + a_r b_s + (a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0) \quad (45)$$

where some first or last few terms should be deleted if $r+s > m$ or $r+s > r$.**(You don't have to worry about this, as you see in the following.)**

By equation (44), we see

$$p|(a_0 b_{r+s} + \cdots a_{r-1} b_{s+1}) \text{ and } p|(a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0) \tag{46}$$

Then by equation (45), and that $p \not| a_r$ and $p \not| b_s$, we see

$$p \not| a_r b_s \text{ which give us } p \not| c_{r+s} \tag{47}$$

If p does not divides c_{r+s}, then p does not divides all $c_0, \cdots, c_{n+m}$. (done)

■

Corollary 20.1. *The finite product of primitive polynomials of $D[x]$ is again primitive.*

Theorem 21. *Let D be a UFD and $\mathbb{F}$ be the field of quotient of D, and let $f(x) \in D[x]$ be a non-constant polynomial.*

$$f(x) \text{ is irreducible} \iff f(x) \text{ is irreducible in } \mathbb{F}[x] \text{ and } f(x) \in D[x] \text{ is primitive} \tag{48}$$

Proof. From right to left it hold true because $D[x] \subseteq \mathbb{F}[x]$.

So we only have to prove from left to right. Notice that by Theorem 19, we have already proven $f(x)$ is primitive. Suppose $f(x)$ is reducible in $\mathbb{F}[x]$ and express $f(x) = r(x)s(x)$, where $r(x), s(x) \in \mathbb{F}[x]$ are non-constant.

Suppose $[d]$ is the least common multiple of $\{[d_i]\}$ where $\{d_i\}$ are denominators of coefficients of $r(x)$ or $s(x)$. Observe

$$(d)f(x) = r_1(x)s_1(x) \tag{49}$$

Where the coefficients of $r_1(x)$ and $s_1(x)$ are respectively the nominator of coefficients of $r(x)$ and $s(x)$. Factorize $f(x), r_1(x), s_1(x)$ in the form

$$f(x) = [c]g(x) \text{ and } r_1(x) = [c_1]r_2(x) \text{ and } r_2(x) = [c_2]s_2(x) \tag{50}$$

Where $[c], [c_1], [c_2]$ are respectively the contents of $f(x), r_1(x), r_2(x)$.

Then we express equation (50) in the form

$$I := [cd]g(x) = [c_1 c_2]r_2(x)s_2(x) \tag{51}$$

Because $r_2(x)s_2(x)$ are primitive, given by Lemma 20, and $g(x)$ are primitive, and contents of I is unique, we see $g(x) = ur_2(x)s_2(x)$ for some unit u.

By $f(x) = [c]g(x)$, we know $f(x) = cu_1 g(x)$ for some unit u_1.

Then $f(x) = (cu_1 u)r_2(x)s_2(x)$ is reducible. ■

Corollary 21.1. *Suppose D is a UFD and $f(x) \in D[x]$*

$$f(x) \text{ is reducible} \iff f(x) \text{ is reducible in } \mathbb{F}[x] \tag{52}$$