PRINCIPAL IDEAL DOMAINS AND UNIQUE FACTORISATION DOMAINS

HRISHABH AYUSH

Abstract. This paper is going to talk about the properties of Principal Ideal Domains, Unique Factorisation Domains and other similar things which are related to this topic such as Integral Domains, Euclidean domains, Field of fractions along with some supported examples.

1. Introduction

Principal Ideal Domain is an integral domain where every proper ideal can be generated by single element. Every Euclidean Ring is a PID, but not conversely. Nevertheless, the notion of greatest common divisor which is obviously from the Euclidean Algorithm can be extended to more general context of PID. Every PID is a unique factorisation domain, but the converse is not true. Every polynomial ring over a field is a UFD, but it's a PID iff the number of indeterminates is one.

2. Principal Ideal Domain

We begin first by introducing Principal Ideal Domain and some of its useful properties:

Definition 2.1. An integral domain D is called a principal ideal domain(PID) if every ideal is principal.

Example. $\mathbb{Z}$, $k[x]$ are two such examples.

Recall. There some results which I will be using to explain the further results.

- For $a \in D$ the principal ideal generated by a is $(a) = \{ra \mid \text{where } r \in D\}$.
- $p \in D$ is said to be irreducible if when $p = ab$, when a or b is a unit.
- $p \in D$ is said to be prime if when $p \mid ab$ we have $p \mid a$ or $p \mid b$.

Lemma 2.2. *Let D be a PID, one has $a \mid b$ if and only if $(b) \subseteq (a)$. Elements a and b are associates iff $(a) = (b)$.*

Proof. Suppose $a \mid b$ then $b = ar$ for some $r \in D$. Let $x \in (b)$ then $x = by$ for some $y \in D$D. We can say that $x = ary \in (a)$ which clearly states that $(b) \subseteq (a)$. Now suppose $(b) \subseteq (a)$, so $b \in (a)$ for some $r \in D$. So we proved $a \mid b$.

Now, let us prove for the part that a and b are associates and $(a) = (b)$. Suppose that a and b are associates $\exists$ a unit $u \in D \implies a = bu \implies b \mid a$, hence $(a) \subseteq (b)$, also $au^{-1} = b$, then $a \mid b$, hence $(b) \subseteq (a) \implies b = ax$ and $a = by$, so combining both of them we get $b = bxy \implies xy = 1$, hence x is a unit and we proved that a and b are associates. ■

Theorem 2.3. *Let D be a PID and $0 \neq (p) \subseteq D$, then (p) is a maximal ideal if and only if p is irreducible.*

Proof. Suppose (p) is a maximal ideal and $p = ab$(Target:a or b is a unit). The equation tells us that $a \mid p$, then by our lemma we have $(p) \subseteq (a) \subseteq D$. Then by the definition of a maximal ideal, we can say $(p) = (a)$ or $(a) = D$. Then in the first case p and a are associates, so b is a unit. Similarly, in the second case we can say that a is a unit(by our lemma). Hence either way we proved that p is irreducible.

Another interesting approach is by supposing p is irreducible. Consider $a \in D$ with $(p) \in (a) \in D$. Notice by our lemma $a \mid p$, so $p = ab$ for some $b \in D$, but p is irreducible so a is a unit or b is a unit. In the first case, $(a) = D$. In the second case, p and a are associates $(p) = (a)$. Hence in both the cases (p) is maximal ideal. ■

Corollary 2.4. *If $p \in D$ is irreducible (D is a UFD), then it is prime. In an arbitrary ring this is not the case, in that case the notion of being a prime is more restricted than the notion of being irreducible.*

Proof. Suppose p is irreducible. Look for what it takes for p to be prime. Then we want to show $p \mid a$ or $p \mid b$. So $ab = pr$ for some $r \in D$ and $ab \in (p)$, a maximal ideal. That implies it is a prime ideal. So, $a \in (p)$or $b \in (p)$.Hence we can say $a = px$ or $b = py$, which clearly states $p \in a$ or $p \in b$. ■

Proposition 2.5. *Every ideal in $k[x]$ is a Principal Ideal domain.*

Proof. Let's suppose k is a field. Then by Division Algorithm we have $\forall f(x), g(x) \in k[x] \exists! q(x), r(x)$ such that $f(x) = g(x).q(x) + r(x)$ with

$$0 \leq \deg r(x) < \deg g(x)$$

Suppose $I \subseteq k[x]$ is an ideal. Take $p(x) \in I$ such that $p(x)$ is monic polynomial and $deg[p(x)]$ is minimal over all polynomials of positive degree. Suppose $f(x) \in I$ and we perform division algorithm such that $f(x) = p(x).q(x) + r(x)$. Here $deg[r(x)]$ must be 0 otherwise it would violate the minimality of $p(x)$, which clearly indicates $f(x) \in (p(x))$ and $I \subseteq (p(x))$. Other case include $p(x) = \alpha \neq 0 \in k$. So that means $(p(x)) = (\alpha) = k[x]$. Hence we proved that $k[x]$ is a PID.

Example. $\mathbb{Z}[x]$ is not a PID. The proof of this example is left as an exercise for the readers. You can start by taking $I = (x, 2)$ and proving that it is not a principal ideal.

■

3. Field of Fractions

We can think of $\mathbb{Q}$ "as a set of symbols $\frac{a}{b}$", where $a, b \in \mathbb{Z}(b \neq 0)$,and $\frac{a}{b} = \frac{c}{d} \implies ad = bc$, here I will be using few notations to prove some results.

- D is any integral domain.
- $S = \{(a, b) \mid \text{where we have } a, b \in D,\ b \neq 0\}$.
- $\sim \subseteq S \times S$, $(a, b) \sim (c, d)$, that implies $ad = bc$.
- $[a, b] = \{(c, d) \in S \mid (a, b) \sim (c, d)\}$, where the square brackets denote equivalence class.
- $F_D = \{[a, b] \mid \text{where } a, b \in D,\ b \neq 0\}$.

Theorem 3.1. *F_D is a field(the field of fractions of D). It is the unique "smallest" field such that $D \hookrightarrow F_D$, which tells that D can be embedded in F_D.*

Proof. First, we try to prove that $\sim$ is an equivalence relation. (Reflexive) $(a,b) \sim (a,b)$ because $ab = ab$. (Symmetry) Suppose $(a,b) \sim (c,d)$, such that we have $ad = bc$ or $bc = ad$. Hence $(c,d) \sim (a,b)$. (Transitive) Let's suppose $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$. So we will get $(a,b) \sim (e,f)$.

Now we will try to prove that addition is well defined in this case. Our motivation is $\mathbb{Q}$ numbers, where it has the property of $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$. So the same thing we see in equivalence class as $[a,b] + [c,d] = [ad + bc, bd]$. Now suppose $[a,b] = [\hat{a}, \hat{b}]$, which completely indicates that $a\hat{b} = \hat{a}b$. Similarly we make the case with c and d and we finally get the result $[a,b] + [c,d] = [ad + bc, bd]$ or $[\hat{a}, \hat{b}] + [\hat{c}, \hat{d}] = [\hat{a}\hat{b} + \hat{c}\hat{d}, \hat{b}\hat{d}]$.

Now we want to show that we can "include" $D \hookrightarrow F_D$. Consider $\iota : D \to F_D$, and also $\mathbb{Z}(a) = [a,1]$. Now we will exhibit it is a ring homomorphism $\iota(a+b) = [a+b,1] \implies [a,1] + [b,1] = \iota(a) + \iota(b)$.

Also $\iota(ab) = [ab,1] = [a,1] + [b,1] = \iota(a)\iota(b)$. Now along with this we prove that a ring homomorphism is injective. Suppose $\mathbb{Z}(a) = 0$. Then we have $[a,1] = [0,1]$, which implies to the fact that $a = 0$. But if anything in the kernel is equal to 0 that tells us that the kernel is just the zero element, which is the same thing as saying it is injective.

Lastly, we try to show the uniqueness of D. So we have $\mathbb{Z} \hookrightarrow \mathbb{R}$ and also $\mathbb{Q} \hookrightarrow \mathbb{R}$. Suppose that we have a field k such that $D \overset{\phi}{\hookrightarrow} F_D$, where ϕ is an injective ring homomorphism. Our goal is to find some $\psi : F_D \to k$ such that $D \overset{\iota}{\hookrightarrow} F_D \overset{\phi}{\hookrightarrow} k$. Set $\psi([a,b]) = \phi(a)(\psi(b))^{-1})$ and we observe that $\phi(a), \phi(b) \in k$. So the last thing we need to check is that ψ is an injective field homomorphism. $\psi([a,b] + [c,d]) = \psi([ad + bc, bd]) = \phi(ad + bc)(\phi(bd))^{-1} = (\phi(a)\phi(d) + \phi(b)\phi(c))(\phi(b))^{-1}(\phi(d))^{-1}$ which after multiplication gives you $\phi(a)\phi(b)^{-1} + \phi(c)\phi(d)^{-1} = \psi[a,b] + \psi[c,d]$.

Similarly, we want to show for the multiplication part. So the final conclusion we would get is $\psi([a,b].[c,d]) = \psi[a,b]\psi[c,d]$. Suppose $[a,b] \in ker\psi$. We want to show that this thing is trivial. In other words it is injective. Thus $\psi[a,b] = 0$ and then $(\phi(a)\phi(b)^{-1} = 0)\phi(b)$. Hence this gives us the result that $\phi(a) = 0$. So, $a = 0$ and $[a,b] = [0,1]$. So the $ker\psi = \{[0,1]\}$. Hence it is injective and therefore we proved this result. ∎

4. Unique Factorisation Domain

Definition 4.1. We say an integral domain D is a Unique Factorisation Domain (UFD) if

- Every nonzero-nonunit can be written as the product of irreducibles.
- If $a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ with p_i, q_j to be irreducible then $r = s$ and $\exists$ a permutation $\sigma \in S_r$ with $p_i = q_{\sigma(i)} u_i$, where u_i is a unit.

We have some important results if we are given with $p(x) = a_n x^n + \ldots + a_0 \in D[x]$

- $content(p(x)) = gcd(a_0, \ldots, a_n)$
- $p(x)$ is primitive if *content* = 1, which means the coefficients of the polynomials have no common factor

Proof. $\mathbb{Z}[\iota\sqrt{3}] = \{a + b\iota\sqrt{3} \mid a, b \in \mathbb{Z}\}$. Consider $4 = 2.2 = (1 + \iota\sqrt{3})$(1-$\iota\sqrt{3}$). For it to be a UFD $2 = (1 + \iota\sqrt{3})$u, where u is a unit. $u = a + b\iota\sqrt{3} \in \mathbb{Z}[\iota\sqrt{3}] \subseteq \mathbb{C}$. $u^{-1} = \frac{a - b\iota\sqrt{3}}{a^2 + 3b^2} \in \mathbb{Z}[\iota\sqrt{3}]$. Then we will need $\frac{a}{a^2+3b^2} \in \mathbb{Z}$. So we will have $b = 0$ and $\frac{a}{a^2} \in \mathbb{Z} \implies \frac{1}{a} \in \mathbb{Z}$. Then $a = \pm 1$.So that implies $u = \pm 1$. Hence $2 = \pm(1 + \iota\sqrt{3})$, which is not true. This is a contradiction to our assumption. ∎

Example. $\mathbb{Z}$ is a UFD by Fundamental theorem of arithmetic. Let's also consider a non example $\mathbb{Z}[\iota\sqrt{3}]$ and also $\mathbb{Z}[\sqrt{5}] \subseteq \mathbb{R}$.

Theorem 4.2 (Gauss's Lemma)**.** *If $f(x), g(x) \in D[x]$ are primitive then so is $f(x).g(x)$*

Lemma 4.3. *$cont(f(x)g(x)) = cont(f(x)).cont(g(x))$*

Lemma 4.4. *Suppose $p(x) \in D[x]$ with $p(x) = f(x).g(x) \in F[x]$, where F is the field of fraction, then $\exists \hat{f}(x), \hat{g}(x)$ such that $p(x) = \hat{f}(x)\hat{g}(x)$*

Corollary 4.5. *If $p(x)$ is irreducible in $D[x]$, then $p(x)$ is also irreducible in $F[x]$, and the converse is also true.*

Theorem 4.6. *If D is a UFD then $D[x]$ is a UFD.*

The proof to this property is left as an exercise for the readers and they can try this out using the previous properties to show the uniqueness and primitive property.

5. Euclidean Domains

Definition 5.1. An integral domain D is known as a Euclidean Domain if $\exists\ N : D \to \mathbb{N}$ such that

- If $0 \neq a, b \in D$ then $N(a) \subseteq N(ab)$.
- If $a, b \in D$ with $b \neq 0$ then there exists $q, r \in D$ such that $a = bq + r$ with $r = 0$ or $N(r) < N(b)$.

Example. $\mathbb{Z}$ which are just given by the following relation $N(m) = |m|$

Example. $k[x]$, the ring of formal power series over the field k. For each nonzero power series P, define $f(P)$ as the order of P, that is the degree of the smallest power of occurring in P. In particular, for two nonzero power series P and Q, $f(P) \leq f(Q)$ if and only if P divides Q.

Nonexample. Every domain that is not a principal ideal domain, such as the ring of polynomials with at least two indeterminates over a field, or the ring of univariate polynomials with integer coefficients, or the number ring $\mathbb{Z}[\sqrt{(-5)}]$.

Definition 5.2. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a Euclidean domain. So this is the property of Gaussian integers.

Proof. Define $N(\alpha) = \alpha\bar{\alpha} = |\alpha|^2$. Then $\alpha = a + bi$ and $\alpha = a - bi$. Then $N(\alpha) = a^2 + b^2$, where $a, b \in \mathbb{Z}$. Now using $\alpha, \beta \in \mathbb{Z}[i] \implies N(\alpha\beta) = \alpha\beta\bar{\alpha}\beta = \alpha\beta\alpha\bar{\bar{\beta}}$. Further rearranging the terms, we get $\alpha\bar{\alpha}\beta\bar{\beta} = N(\alpha)N(\beta) \geq N(\alpha)$. Now we move on to prove the second property. So suppose $\alpha\beta \in \mathbb{Z}[i]$, where $\beta \neq 0 . \alpha = a + bi, \beta = c + di \implies \beta^{-1} = \frac{c-di}{c+di} = \frac{\bar{\beta}}{|\beta|^2}$. Hence, we find that

$$\begin{aligned}
\alpha\bar{\beta}^{-1} &= \frac{(a+bi)(c-di)}{c^2+d^2} \\
&= \frac{1}{c^2+d^2}((ac+bd)(bc-ad)i) \\
&= \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i \\
&= (q_1 + r_1) + (q_2 + r_2)i
\end{aligned}$$

where $-\frac{1}{2} \leq r_1, r_2 \leq \frac{1}{2}$ and $q_1, q_2 \in \mathbb{Z}$.

$$\begin{aligned}
&\alpha\beta^{-1} = (q_1 + r_1) + (q_2 + r_2)i \\
&= (q_1 + q_2 i) + (r_1 + r_2 i) \\
&\alpha = \beta\gamma + \beta(r_1 + r_2 i) \\
&\alpha = \beta\gamma + \rho \\
&\therefore N(\rho) = \beta\bar{\beta}(r_1 + r_2 i)(r_1 - r_2 i) \\
&= N(\beta)(r_1^2 + r_2^2), 0 \leq r_1^2, r_2^2 \leq \frac{1}{4} \leq \frac{1}{2}N(\beta) < N(\beta)
\end{aligned}$$

Here we finished our proof, which is in fact a Euclidean Domain. ■

Theorem 5.3. *If D is a Euclidean Domain then it is indeed a PID.*

Proof. Suppose $I \subseteq D$ is an ideal. Take b$\in I$ such that $N(b)$ is minimal among all elements from $I(b \subseteq I)$. Now, take $a \in I$ and by Division Algorithm, $a = bq + r$, where $r = 0$, or $N(r) < N(b)$. Also if we see $r = a - bq \in I$, we will have $r = 0$, otherwise we would contradict the minimality of $N(b)$.

$$a = bq \in (b) \implies I \subseteq (b) \implies I = (b)$$

■

6. Ideals of quotients of PIDs

Theorem 6.1 (Fourth Isomorphism Theorem)**.** *Let $f : G \longrightarrow G'$ be a surjective homomorphism. Then*

- *There is an inclusion preserving bijection*
$$\{A \mid Kerf \leq A \leq G\} \longrightarrow \{B \mid B \leq G\}$$
given by $A \longmapsto f(A)$ with inverse given by $B \longmapsto f^{-1}(B)$
- *Let $Kerf \leq N \leq G$. Then $N \trianglelefteq G$ if and only if $f(N) \trianglelefteq G'$ in which case there is an isomorphism $G/N \longrightarrow G'/f(N)$ given by $aN \longmapsto f(a)f(N)$ for all $a \in G$*

Proof. We sketch a proof. As for the first part, we suppose that $f : G \longrightarrow G'$ is any homomorphism. Then $Kerf \subseteq f^{-1}(B)$ and $B \subseteq f(f^{-1}(B))$ for all $B \leq G'$. If f is surjective then $= f(f^{-1}(B))$. Let $A \leq G$. Then A$\subseteq f^{-1}(f(A))$. If $Kerf \subseteq A$ then $A = f^{-1}(f(A))$. As for second part, observe that the composite $G \longrightarrow G' \longrightarrow G'/f(N)$ of f followed by the projection is surjective and has kernel $f^{-1}(f(N)) = N$, by the first Isomorphism Theorem. ■

Theorem 6.2 (Zorn's Lemma)**.** *Every poset with the property that every increasing chain has a maximal element has a maximal element for the whole part.*

Example. Let S be the set of all subgroups of a given group G. For $H, K \in S$ (that is, H and K are subgroups of G), declare $H \leq K$ if H is a subset of K. This is a partial ordering, called ordering by inclusion. It is not a total ordering: for most subgroups H and K neither $H \subset K$ nor $K \subset H$. One can similarly partially order the subspaces of a vector space or the ideals (or subrings or all subsets) of a commutative ring by inclusion

Example. In $\mathbb{R}$ with its natural ordering, the subset $\mathbb{Z}$ has no upper bound while the subset of negative real numbers has the upper bound 0(or any positive real). No upper bound on the negative real numbers is a negative real number.

Lemma 6.3. *Let S be a partially ordered set. If $\{s_1, \ldots, s_n\}$ is a finite totally ordered subset of S then there is an s_i such that $s_j \leq s_i$ for all $j = 1, \ldots, n$.*

Proof. The $s_i's$ are all comparable to each other; that's what being totally ordered means. Since we're dealing with a finite set of pairwise comparable elements, there will be one that is greater than or equal to them all in the partial ordering on S. The reader can formalize this with a proof by induction on n, or think about the bubble sort algorithm. ■

Proposition 6.4. *Suppose D is a PID and $I \subseteq D$ is an ideal then every ideal of D/I is principal.*

Proof. Supppose $\overline{J} \subseteq D/I$ is an ideal. $\overline{J} = J/I$ with $I \subseteq J \subseteq D$. Since D is a PID $I \subseteq (a)$ and $J \subseteq (b)$. So the claim is $\overline{J} = (b + I)$. So $(b + I) \subseteq \overline{J}$ is very much true because $b + I \in (b) + I$. Suppose $x \in \overline{J} = J/I = (b)/I = \{j + I \mid j \in (b)\}$. We can say $x = rb + I$ for some $r \in D$. So $x = (r + I)(b + I) \in (b + I)$. Hence, $\overline{J} \subseteq (b + I)$. ■

Corollary 6.5. *If $P \subseteq D$ is a prime ideal then D/P is a PID.*

Proof. We have D/P is a principal ring by the example. So D/P is an integral domain because P is prime. ■

Example. If D is a PID. Then every prime ideal contained in D is maximum.

Example. Let D be an integral domain such that every prime ideal is principal then D is a PID.

Proof. We are going to prove by the method of contradiction. Suppose we have a set of non principal ideals $A = \{I \subseteq D \mid I \text{ is not principal}\}$.

This is a poset with the ordering $I \subseteq I'$. Consider a chain of $I_1, I_2, I_3, \ldots \in A$ with $I_1 \subseteq I_2 \subseteq I_3 \ldots$ So consider $I_\infty = \bigcup_{i=1}^{\infty} I_i$. Our claim is $I_\infty \in A$.Suppose not $I_\infty = (a)$. So $a \in I_\infty$. Hence $a_n \in I_n$ for some n. $(a) \subseteq I_n \subseteq I_\infty = (a)$. Therefore we have $I_n = (a)$. We have satisfied the hypothesis of Zorn's Lemma that A has a maximal ideal. Now, we consider I is the maximal non-principal ideal. I is not a prime ideal and $\exists a, b \in D$ such that $ab \in I$ but $a \notin I$ and $b \notin I$. Observe $I \subsetneq (I, a) = (\alpha)$. The fact that (α) is a PID is by maximality of I. Also $I \subsetneq (I, b) \subseteq J = \{r \in D \mid ra \in I\} = (\beta)$. Same is the reason for this case too by maximality of I. Now taking $x \in I \subseteq (\alpha)$, so $x = r\alpha$, for some r$\in D$. Now $r(\alpha) \subseteq (x) \subseteq I \implies a \in (\alpha) \implies r\alpha \in I \implies r \in J$, so we have $r = y\beta \implies x = y(\alpha\beta) \in (\alpha\beta) \implies I \subseteq (\alpha\beta)$. Here one point from the proof must be noted that $\beta \in J \implies \beta\alpha \in J$. Since $I \subset D$ is an ideal $i\beta \in I$ $\forall i \in I$. That tells us for any $s \in (Ia)$ we have $\beta s \in I$. In particular we take $s = \alpha \implies \alpha\beta \subset I \implies (\alpha\beta) \subseteq I$. But this is a contradiction, therefore D is a PID and hence our assumption was wrong. ■

References

[1] Austin Alderete. Principal ideal domains. In *Notes Field*, 2018.

[2] A. W. Chatters, M. P. Gilchrist, and D. Wilson. Unique factorisation rings. *Proceedings of the Edinburgh Mathematical Society*, 35(2):255–269, 1992.

[3] Allan Clark. *Elements of abstract algebra*. Courier Corporation, 1984.

[4] Veselin Peric and Mirjana Vukovic. Some examples of principal ideal domain which are not euclidean and some other counterexamples. *Novi Sad J. Math*, 2008.

[5] Elliot S. Wolk. On the principle of dependent choices and some forms of zorn's lemma. *Canadian Mathematical Bulletin*, 26(3):365–367, 1983.

[6] Conan Wong. On a principal ideal domain that is not a euclidean domain. In *International Mathematical Forum*, 2013.