RINGS

Cosets

Author
Tom Jeong

November 6, 2024

Contents

1 prime elemnets unique factorization domains. **3**

2 principle ideal domains and UFD **4**

1 prime elemnets unique factorization domains.

exercise show that the field of fractions of $\mathbb{Z}(i)$ is $\mathbb{Q}[i]$

Definition 1.1.

1. A non-zero element in $x \in R - R^*$ Has a factorization into irreducible element if $\exists$ irreducible elements

$$p_1, p_2, \ldots, p_n \in R$$

such that $x = p_1 p_2 \ldots p_n$

2. We say x has a unique factorization into irreducible elements if for any other irreducieble factorization

$$x = q_1 q_2 \ldots q_n$$

Every $p_i, i = 1, \ldots n$ divides some q_j for some $j = 1, \ldots, m$

remark Since q_i is irreducible, $q_i \mid q_j$ implies $q_j = up_i$ for some $u \in R^*$ therefore n = m

Definition 1.2. A domain R such that every nonzero element in $R - R^*$ has a unique facrotization into irreducible elements is called a unique factorization domain UFD

Definition 1.3. A Nonzero element $p \in R - R^*$ is called a prime element if $p \mid xy \to p \mid x \vee p \mid y$

exercise If p is prime and $p \mid x_1 x_2 \ldots x_n$, then $p \mid x_1$ for some $i = 1 \ldots, n$

Proposition 1.1. (3.5.2)
A prime element is irreducible h

Proof. let $p \in R - R^*$ be prime
If $p \mid xy$, then $p \mid x$ or $p \mid y$
wlog $p \mid x$
Then $x = rp$ for some $r \in R$
Then $p = rpy$ AND since R is a domain we can cancel. thus $1 = ry$
Hence, y is a unit so p is irreducible □

example

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\} \subset \mathbb{C}$$
$$6 = (1 - \sqrt{-5})(1 + \sqrt{5})$$
Claim: $2 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible but no prime

Proof. 1. 2 is not prime:
$2 \mid (1 - \sqrt{-5})(1 + \sqrt{5})$ but 2 does not divide $1 - \sqrt{-5}$ nor $1 + \sqrt{-5}$

since $\frac{1}{2} \pm \frac{\sqrt{-5}}{2} \notin \mathbb{Z}[\sqrt{-5}]$
2. 2 is irreducible

$$\begin{aligned} &N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{N} \\ &N(z) = z\bar{z} \\ &N(a + b\sqrt{-5}) = a^2 + 5b^2 \end{aligned}$$

$z \in \mathbb{Z}[\sqrt{-5}]^* \leftrightarrows N(z) = 1$
Then $a + b\sqrt{-5}$ is a unit $\leftrightarrows a = \pm 1, b = 0$
Let

$$\begin{aligned} &2 = xy \\ &\quad \text{where } x = a + b\sqrt{-5} \\ &y = c + d\sqrt{-5} \\ \text{Then } N(2) &= 4 = N(x)N(y) \\ &= (a^2 + 5b^2)(c^2 + 5d^2) \\ &= a^2c^2 + 5a^2d^2 + 5b^2c^2 + 25b^2d^2 \\ &\text{therefore,} \\ &4 = a^2c^2 \text{ and } b = d = 0 \\ &ac = \pm 2 \text{ so a or c is } \pm 1 \end{aligned}$$

So x, or y is a unit ☐

2 principle ideal domains and UFD

Goal: we will show that every PID is a UFD (the converse is not true)
example $\mathbb{R}[x, y]$ = {polynomials in x and y with real coefficients} is a UFD but is not a PID

$$I =< x, y >$$

is not principal

Lemma 2.1 (3.5.5)**.** Let R be a PID and $r \in R$ a non zero element, Then r has an irreducible factorization.

Claim: IF $< a_1 >\subseteq< a_2 >\subseteq \cdots \in R$ where R is a PID, Then

$$\exists N \in \mathbb{N}$$

such that $< a_i >=< a_{i+1} > \forall i > N$

proof of claim.
in the HW we shouwed that the

$$\mathbb{U}_{i=1}^{\infty} < a_i >$$

is an ideal
since R is a PID,

$$\Cup_{i=1}^{\infty} < a_i >=< d >$$

for some $d \in R$
Thus $d \in < a_N >$ for some N , and so $< d > \subseteq < a_N >$ and hence $< a_i >=< d >$ for $i \geq N$
Suppsoe $r \in R - R^*$ is a non zero element which is not a product of irreducible. then

$$r = a_1 b_1, a_1, b_1 \notin R^*$$

where at least one of a_1, b_1 is not a product of irreducibles.
WLOG a_1 is not a product of irreducibles.
Then $a_1 = a_2 b_2, a_2, b_2 \notin R^*$ where at least of a_2, b_2 is not a product of irreducibles ..
Then

$$< R > \subsetneq < a_1 > \subsetneq < a_2 > \subsetneq < a_3 > \subsetneq \dots$$

which contradicts the claim hence rm ust have an irreducible factorization.

□

Proposition 2.2 (3.5.6)**.**
suppose R is a PID that is not a field. An ideal $< x > \subset R$ is a Maximal Ideal IFF x is irreducible.

Proof.

1. $\rightarrow$ Assume $< x >$ is a maximal and $x = ab$, we want to show that a or b is a unit.

$$\begin{aligned} &\text{Assume neither } a \text{ or } b \text{ is a unit} \\ &\text{Then } < x > \subsetneq < a > \text{ since } b \text{ is not a unit} \\ &< x > \subsetneq < b > \text{ since } a \text{ is not a unit} \end{aligned}$$

   contradicting maximaility of $< x >$ hence a or b must be a unit

2. $\leftarrow$ Suppose x is irreducible.

$$\begin{aligned} &\text{IF } < x > \subseteq < y > \text{ then} \\ &x = \lambda y \text{ for some } \lambda \in R \\ &\text{since } x \text{ is irreducible} \\ &\lambda \text{ or } y \text{ is a unit} \\ &\text{If } \lambda \text{ is a unit, then } < x >=< y > \\ &\text{If } y \text{ is a unit, } < y >= K \\ &\text{Hence } < x > \text{ is maximal.} \end{aligned}$$

□

Theorem 2.3 (3.5.7)**.** A PID R is a UFD

Proof. By lemma 3.5.5 since R is PID, irreducible factorization exists. We need to show uniqueness. We will show that irreducibility elemens are prime and then apply Prop 3.5.3 to show that R is a UFD

□

> **Proposition 2.4** (3.5.3)**.** Let R be a ring where every non-zero element $r \in R - R^*$ has a factorization into irreducibles. Every irreducible element is a prime element in R iff R is a UFD

Proof.

1. $\rightarrow$ Suppose $x \in R - R^*$ with $x = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$ wher pi qj are irreducible.

2. $\leftarrow$ Let R be a ufd and $p \in R$ irreducible. Suppose $p \mid xy$ since R is a UFD, x and y each have unieque factorizations and by uniqueness one of these factorizations must have an irreducible factor that is divisible by p.
   Hence $p \mid x$ or $p \mid y$ so p is prime.

□

To see that every PID is a UFD we will show that irreducible elements are prime and apply prop 3.5.3 to show R is a UFD.
Let $p \in R$ p irreducible, with $p \mid ab$ and $p \nmid a$
WTS $p \mid b$
since $p \nmid a, a \notin < p >$
Then, $< p > \subsetneq < a, p >$
Since p is irreducible, $< p >$ is maximal by te earlier prop 3.5.6
Hence $< a, p >= R$ so exists $x, y \in R$ so that xa + yp = 1
Multiplying both sides by b: $xab + ypb = b$
Since $p \mid ab$, it follows that $p \mid b$