Contents

Chapter 1

Unique Factorization

1.1 Class Notes 17-01-12

For us, ring means commutative ring with identity.

Definition 1.1.1 A *ring* is a set with two binary operations $(+, \cdot)$ satisfying

1. $(R, +)$ is an *abelian group*, which means
   - $+$ is commutative and associative.
   - $\exists\ 0_R, a + 0_R = 0_R + a$ for all $a \in R$.
   - Given $a \in R$, $\exists a' \in R$ such that $a + a' = 0_R$.
2. $\cdot$ is commutative and associative.
   $\exists\ 1_R$ such that $a \cdot 1_R = 1_R \cdot a = a$ for all $a \in R$.
3. $\cdot$ is distributive over addition, which means
   - $a \cdot (b + c) = a \cdot b + a \cdot c$
   - $(a + b) \cdot c = a \cdot c + b \cdot c$

Exercise 1.1.1

1. Show that $a + b = a + c \Rightarrow b = c$.(Cancellation)

   Proof.

   $$\begin{aligned} a + b = a + c &\Leftrightarrow a' + (a + b) = a' + (a + c) \\ &\Leftrightarrow (a' + a) + b = (a' + a) + c \\ &\Leftrightarrow 0_R + b = 0_R + c \\ &\Leftrightarrow b = c \end{aligned}$$

   ∎

2. Show a' is unique. We denote this a' by $-a$.

   Proof. if the statement doesn't hold, then there exist a', a'' such that $a + a' = 0_R = a + a''$. We then apply cancellation and get $a' = a''$. ∎

3. Show 0_R is unique.

   Proof. Say there are two zero element 0_R and $0'_R$, then we have

   $$0_R = 0_R + 0'_R = 0'_R$$

   ∎

4. Show 1_R is unique.

Proof. Say there are two unit element 1_R and $1'_R$, then we have

$$1_R = 1_R \cdot 1'_R = 1'_R$$

■

5. Show $a \cdot 0_R = 0_R \cdot a = 0_R$

   Proof. We know that $a \cdot 0_R + a = a \cdot (0_R + 1_R) = a \cdot 1_R = a = 0_R + a$, apply cancellation then we are done. ■

6. Show that $(-1_R) \cdot a = -a$.

   Proof. Since $a \cdot 0_R = 0_R$, we have $a \cdot (1_R + (-1_R)) = 0_R$ or $a + (-1_R) \cdot a = 0_R$. Then $-a = (-1_R) \cdot a$, for a' is unique. ■

7. The zero ring is the ring with 1 element. Show R is zero ring $\Leftrightarrow 1_R = 0_R$.

   Proof.
   " $\Rightarrow$ " : Trivial.
   " $\Leftarrow$ " : Since we have $a \cdot 1_R = 1_R \cdot a = a$ for all $a \in R$ and $1_R = 0_R$, we have $0_R = a \cdot 0_R = a$ for all $a \in R$. ■

8. Does cancellation hold for $\cdot$?
   Sol. No. Consider $a \cdot b = a \cdot c$ and $a \neq 0_R$, then $a \cdot (b - c) = 0_R$. So if R is an *integral domain*, then we can apply cancellation of non-zero element.

Definition 1.1.2 R is said to be an *integral domain* if

$$a \cdot b = 0 \quad \Longleftrightarrow \quad a = 0 \;\text{ or }\; b = 0.$$

Definition 1.1.3 R is said to be a field if every non-zero element in R has a multiplication inverse.

Exercise 1.1.2

1. If R is an integral domain, then we can apply cancellation of non-zero element.
2. Show that every field is an integral domain.

   Proof. If $a \cdot b = 0$ and $a \neq 0_R$, let a' be the multiplication inverse of a, then $b = 1_R \cdot b = a' \cdot a \cdot b = a' \cdot 0_R = 0$. ■

3. Check that a^{-1} is unique.

   Proof. If a^{-1} and a' are both multiplication inverse of a, then $a \cdot a^{-1} = a \cdot a' = 1_R$. Apply cancellation of non-zero element, we have $a' = a^{-1}$. ■

Remark 1.1.1 Though every field is an integral domain, not every integral domain is a field. For example, $\mathbb{Z}$ is an integral domain but not a field.

Ways to make new rings:

Let R be an integral domain, how to construct a new ring?
Let $K = \{(a, b), a, b \in R, b \neq 0\}$. We also define an equivalent relation $(a, b) \sim (c, d)$ if $ad = bc$.

- Check this is an equivalent class.
  - $(a, b) = (a, b)$
  - if $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, then $(a, b) \sim (e, f)$
- We define

- $(a,b)+(c,d)=(ad+bc.bd)$
- $(a,b)\cdot(c,d)=(ac,bd)$

Check these two operation pass to equivalent class.

- $0_K=[(0,1_R)]$, $1_K=[(1_R,1_R)]$

Definition 1.1.4 If R,S are two rings, a homomorphism $\phi:R\to S$ is a map such that
1. $\phi(1_R)=1_S$.
2. $\phi(a+b)=\phi(a)+\phi(b)$.
3. $\phi(ab)=\phi(a)\phi(b)$.

An isomorphism is a homomorphism that is both injective and surjective.

$\phi:R\to S$, $a\mapsto[(a,1_R)]$ is an injective homomophism. For example, we have $\mathbb{Z}\subset\mathbb{Q}$.

Remark 1.1.2 If R is a field, then the homomorphism is isomorphism, i.e., ϕ is also surjective. Because for any $[(a,b)]\in K$, we have $\phi(ab^{-1})=[(ab^{-1},1)]=[(a,b)]$.

Ways to kill elements:

Definition 1.1.5 An ideal I in R is a non-empty subset such that
1. I is closed under addition.
2. I is closed under multiplication by arbitrary elt in R.

Note that $(I,+)\subset(R,+)$ is an abelian subgroup.

Example 1
- (0) is an ideal.
- R itself is an ideal.
- if $a\in R$, the $R\cdot a$ is an ideal, denoted by $(a)_R$.
- $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$.

Quotient Ring: Let $I\subset R$ be an ideal. $R/I=$ coset of I in $R=\{a+I,a\in R\}$, we define
1. $(a+I)\oplus(b+I)=(a+b)+I$.
2. $(a+I)\odot(b+I)=ab+I$.

with zero elt $(0+I)$ and identity elt $(1+I)$.

1.2 Unique Factorization in $\mathbb{Z}$

It will be more convenient to work with $\mathbb{Z}$ rather than restricting ourselves to the positive integers. The notion of divisibility carries over with no difficulty to $\mathbb{Z}$. If p is a positive prime, $-p$ will also be a prime. We shall not consider 1 or -1 as primes even though they fit the definition. This is simply a useful convention. They are called the units of $\mathbb{Z}$.
There are a number of simple properties of division that we shall simply list.
1. $a|a, a\neq 0$.
2. If $a|b$ and $b|a$, then $a=\pm b$.
3. If $a|b$ and $b|c$, then $a|c$.
4. If $a|b$ and $a|c$, then $a|(b+c)$.

Lemma 1 Every nonzero integer can be written as a product of primes.

Theorem 1.2.1 For every nonzero integer n there is a prime factorization
$$n=(-1)^{\varepsilon(n)}\prod_p p^{a(p)},$$
with the exponents uniquely determined by n. In fact, we have $a(p)=\mathrm{ord}_p n$.

The proof if this theorem if is not as easy as it may seem. We shall postpone the proof until we have established a few preliminary results.

Lemma 2 If $a, b \in \mathbb{Z}$ and $b \geq 0$, there exist $q, r \in \mathbb{Z}$ such that $a = qb + r$ with $0 \leq r < b$.

Definition 1.2.1 If $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, we define $(a_1, a_2, \ldots, a_n)$ to be the set of all integers of the form $a_1x_1 + a_2x_2 + \cdots + a_nx_n$ with $x_1, x_2, \ldots, x_n \in \mathbb{Z}$.

Remark 1.2.1 Let $A = (a_1, a_2, \ldots, a_n)$. Notice that the sum and difference of two elements in A are again in A. Also, if $a \in A$ and $r \in \mathbb{Z}$, then $ra \in A$, i.e., A is an ideal in the ring $\mathbb{Z}$

Lemma 3 If $a, b \in \mathbb{Z}$, then there is a $d \in \mathbb{Z}$ such that $(a, b) = (d)$

Definition 1.2.2 Let $a, b \in \mathbb{Z}$. An integer d is called a greatest common divisor of a and b if d is a divisor of both a and b and if every other common divisor of a and b divides d.

Remark 1.2.2 The gcd of two numbers, if it exists, is determined up to sign.

Lemma 4 Let $a, b \in \mathbb{Z}$. If $(a, b) = (d)$ then d is a greatest common divisor of a and b.

Definition 1.2.3 We say that two integers a and b are relatively prime if the only common divisors are ± 1, the units.

It's fairly standard to use the notation (a, b) for the greatest common divisor of a and b. With this convention we can say that a and b are relatively prime if $(a, b) = 1$.

Proposition 1.2.2 Suppose that $a|bc$ and that $(a, b) = 1$. Then $a|c$.

Corollary 1.2.3 If p is a prime and $p|bc$, then either $p|b$ or $p|c$.

Corollary 1.2.4 Suppose that p is a prime and that $a, b \in \mathbb{Z}$. Then $\text{ord}_p ab = \text{ord}_p a + \text{ord}_p b$.

1.3 Class Notes 17-01-12

Definition 1.3.1 A non-zero element in $\mathbb{R}$ is called a unit if $\exists\, v \in \mathbb{R}$ such that $uv = 1_{\mathbb{R}}$.

Definition 1.3.2 Two element $a, b \in \mathbb{R}$ are said to be associative if $\exists\, a \in \mathbb{R}$ such that $a = bu$, denoted by $a \sim b$.

Definition 1.3.3 A non-zero element π in $\mathbb{R}$ is said to be irreducible if π is not a unit and if $a|\pi \Rightarrow a$ is a unit or a is associative of π.

Definition 1.3.4 A non-zero element in $\mathbb{R}$ is said to be prime if π is not a unit and $\pi|ab \Rightarrow \pi|a$ or $\pi|b$, $\forall a, b \in \mathbb{R}$.

Proposition 1.3.1 If π is a prime, then π is irreducible.

Proof. Let π be a prime, suppose $a|\pi$, then $\pi = ab$ for some $b \in \mathbb{R}$. Thus $\pi|ab$ and by definition, $\pi|a$ or $\pi|b$.

- If $\pi|a$, then $a \sim \pi$.
- If $\pi|b$, then $a \sim 1$.

∎

Remark 1.3.1 A irreducible is not necessary to be a prime.
Let $R = \mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$. We have

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

We write $\pi = (1 + \sqrt{-5})$ and claim that $2, 3, \pi, \overline{\pi}$ are irreducibles but none of them are associative of each other.
We define the norm function $N : R \to \mathbb{Z}$, where $N(\alpha) = \alpha\overline{\alpha}$, i.e., if $\alpha = a + bi$, then $N(\alpha) = a^2 + 5b^2$. We notice that

- If $\alpha > 0$, then $N(\alpha) > 0$.
- $N(\alpha\beta) = N(\alpha)N(\beta)$.

Check: 2 is irreducible:
Find unit:
$N(uv) = N(1) = 1 = N(u)N(v) \Rightarrow N(u) = N(v) = 1$. But $a^2 + 5b^2 = 1 \Rightarrow a = \pm 1, b = 0$.
Suppose $2 = \alpha\beta$, then $4 = N(2) = N(\alpha\beta) = N(\alpha)N(\beta)$.

1. If $N(\alpha) = 1, N(\beta) = 4$
   Then α is a unit $\Rightarrow$ 2 is irreducible.
2. If $N(\alpha) = 2, N(\beta) = 2$
   Then $a^2 + 5b^2 = 2$ has no solution.

Definition 1.3.5 An UFD (Unique Factorization Domain) is an integral domain R in which every non-zero element(up to unit) factors uniquely into a product of irreducibles.

Proposition 1.3.2 Let R be a domain in which factorization (of irreducibles) exists. Then R *is a UFD* $\Leftrightarrow$ *every irreducible in* R *is prime.*

Proof.
" $\Leftarrow$ " : Let a be an element of R and $a \neq 0$. If $a = \pi_1\pi_2 \cdots \pi_n = \sigma_1\sigma_2 \cdots \sigma_m$ are two factorizations. Since π_1 is prime, $\pi_1 | \sigma_i$ for some i. By rearranging, we may assume $\pi_1 | \sigma_1$, Thus $\pi_1 \sim \sigma_1$. Repeating this process, we can conclude that the two factorizations are the same.

********Not Complete********

■

Remark 1.3.2 There are clearly rings such that no factorization exists. For example, consider the ring $\mathbb{Z}[2^{1/2}, 2^{1/4}, 2^{1/8}, \ldots] \subset \mathbb{R}$. It's the smallest subring of $\mathbb{R}$ that contains $2^{1/2}, 2^{1/4}, \ldots$.

Definition 1.3.6 A ring R is said to be noetherian if it satisfies any of the following equivalent conditions:

1. Any ascending chain of ideals in R terminates.
   Namely, $I_1 \subset I_2 \subset I_3 \subset \cdots \Rightarrow I_n = I_{n+1} = \cdots$ for some n.
2. Any ideal I in R is finite generated.
   Namely, $I = (a_1, \ldots, a_n)$ for some n.

Proof.
"1. $\Rightarrow$2. ": Let I be an ideal, if $I \neq 0$, pick $a_1 \in I, a_1 \neq 0$, clearly $(a_1) \subset I$. If $(a_1) = I$, we are done, If not, $\exists a_2 \in I \backslash (a_1) \Rightarrow (a_1, a_2) \subset I$, this chain terminates.
"1. $\Leftarrow$2. ": Suppose $I_1 \subset I_2 \subset \ldots$ be an ascending ideal. Let $I = \cup I_n$, we claim that I is an ideal. Let $a, b \in I$, then there exists n such that $a, b \in I_n$. Therefore $a + b \in I_n$, and $a + b \in I$. Let $a \in I$, then $a \in I_n$ for some n. Therefore $ra \in I_n \implies ra \in I$. Thus I is an ideal. But $I = (a_1, \ldots, a_m)$, so there exists n, such that $a_1, \ldots, a_m \in I_n$. Thus $I = I_n$ and $I_n = I_{n+1} = \cdots$. ■

Exercise 1.3.1 Suppose R is a Noetherian domain, show R admits factorizations.

Proof. If b is not irreducible, then $b = ac$ or $(b) \subset (a)$

********Not Complete********

■

Definition 1.3.7 A PID (Principle Ideal Domain) is a domain in which every ideal is generated by a single element.

Theorem 1.3.3 Every PID is a UFD.

Proof. Let R be a PID, then it's noetherian. So factorizations exist. So it suffices to show that every irreducible is a prime. Let π be a irreducible in R. Suppose $\pi \mid ab$ and a is not divided by π. We look at $I = (a, \pi)$, there exists $c \in R$, such that $I = (c)$. Thus we have $c \mid \pi, c \mid a$. So $c \sim 1$ or $c \sim \pi$. Since c is not associative of π, c is associative of 1. But then

$$1 = ax + \pi y$$

for some $x, y \in R$. So $b = abx + \pi by$ or $\pi \mid b$. ■